



# **DOMAIN NAME SYSTEM**

## **Security Checklist**

**Version 4, Release 1.7**

**15 August 2009**

**Developed by DISA for the DoD**

**UNCLASSIFIED**

**Unclassified UNTIL FILLED IN**

**CIRCLE ONE**

**FOR OFFICIAL USE ONLY** (mark each page)

**CONFIDENTIAL and SECRET** (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist

Confidential System = CONFIDENTIAL Checklist

Secret System = SECRET Checklist

Top Secret System = SECRET Checklist

## TABLE OF CONTENTS

<b>1. INTRODUCTION.....</b>	<b>1</b>
1.1 Scope of a Review .....	1
1.2 Organization of the Checklist .....	1
1.3 VMS Procedures .....	2
1.3.1 Registering and Managing DNS Assets.....	2
1.3.1.1 Creating Non-Computing DNS Policy Assets .....	3
1.3.1.2 Creating Computing DNS Assets .....	3
1.3.1.3 Asset Finding Maintenance.....	4
1.3.1.4 Verify All Required Assets are Updated .....	4
1.3.2 Printing Compliance and Summary Reports.....	5
1.3.2.1 VC06 Asset Compliance Report.....	5
1.3.2.2 VC03 Severity Summary Report .....	5
1.3.2.3 ASO1 Report.....	5
1.3.2.4 VL03 Report .....	5
<b>2. DNS POLICY CHECKS – APPLIES TO ALL DNS ARCHITECTURES .....</b>	<b>6</b>
<b>3. ALL WINDOWS OS AND UNIX OS DNS PLATFORMS (BIND AND WINDOWS DNS) .....</b>	<b>40</b>
<b>BIND RUNNING ON UNIX OR WINDOWS OS .....</b>	<b>88</b>
3.1 BIND on UNIX Only.....	110
3.2 BIND on Windows Only .....	119
<b>4. WINDOWS DNS.....</b>	<b>127</b>
<b>5. CISCO CONTENT SWITCH.....</b>	<b>142</b>
<b>6. SUMMARY OF CHANGES.....</b>	<b>150</b>

This page is intentionally left blank.

## **1. INTRODUCTION**

This document contains procedures that enable qualified personnel to conduct Domain Name System (DNS) certification or Compliance Validation reviews, or a site self assessment. The DNS review assesses an organization's compliance with the DNS Security Technical Implementation Guidance (STIG). DISA Field Security Operations (FSO) conducts Certification reviews, Security Test and Evaluation, and Enhanced Compliance Validations to provide DISA, Combatant Commands, and other Department of Defense (DoD) agencies and organizations with a level of confidence that their DNS servers and infrastructure are secure and can adequately support their mission.

### **1.1 Scope of a Review**

The primary objective of a DNS review is to examine the site's administrative practices, name servers, and the zones these name servers support. The review should cover not only the authoritative name servers, but all supporting name servers as well. In some cases, this may not be feasible (e.g., the name server is remotely located), however, if any server supporting a zone is not assessed, this should be clearly documented in the final assessment report.

Organizations may also have several caching name servers – i.e., servers that can resolve client queries, but which are not authoritative for any DNS records. These are the servers that are listed in the DNS configuration of the computers on the internal network. A DNS review should also evaluate all of the organization's caching name servers, but a sample may suffice if there are resource or time constraints.

Client DNS configuration is outside the scope of the review, which focuses on DNS servers and related administrative, technical and physical controls.

### **1.2 Organization of the Checklist**

This checklist is arranged by asset posture. The first section is dedicated to the Non-Computing Asset posture of DNS Policy. These checks/requirements need only be performed once for the site as they apply to all DNS servers and the DNS architecture, regardless of platform or function. The finding status should be updated if a change takes place on the system, during a yearly accreditation visit if vulnerabilities are identified, or during a self assessment. The remaining sections focus on the computing asset posture of the type of DNS software running on the platform: All DNS servers, BIND, Windows DNS, or CISCO CSS.

- Section 2: Non-Computing DNS Policy
- Section 3: All DNS servers
- Section 4: BIND servers, both UNIX and Windows operating system platforms
- Section 5: Windows DNS Server
- Section 6: CISCO CSS DNS

## 1.3 VMS Procedures

When conducting a DNS Review, the Team Lead and the assigned Reviewer identify security deficiencies, provide data from which to predict the effectiveness of proposed or implemented security measures associated with the DNS system and operating environment. Security Reviews of a DoD DNS system requires that the results of the review be tracked using the VMS database. The Team Lead begins by completing both the Visit and the Visit Summary forms under the appropriate Organization in VMS. During a site review, Reviewers update findings for a requested set of site assets. Reviewers enter findings in VMS by updating the same compliance status screens used by the site's System Administrators (SAs). For DNS assets, Reviewers will update assets and findings manually using the VMS screen (or the MERT tool) rather than using an XML script (until such time that a script is written). When the Reviewer is finished updating the finding results associated with each asset, the Team Lead will compile an executive summary, finalize the Visit information screen in VMS, and request visit approval. Following a review, the Team Lead reports the results back to the appropriate parties. After reviewing the results of the Visit, the site can then access VMS to provide any required approvals, or POA&M updates.

### 1.3.1 Registering and Managing DNS Assets

In VMS, an asset is defined as a hardware device or an operating system image that hosts an application (or workload) that is accessed by more than one user. An asset may also include physical locations or other non-computing assets, such as a DNS Policy. Unclassified asset components are registered in VMS via the NIPRNet and confidential or secret asset components are registered via the SIPRNet. Both the Reviewer and the SA will create, maintain, and track assets in VMS. The reviewer will use the Asset and Finding Maintenance screen to perform these functions. The SA will use the By Location navigation chain to perform the same function. When Reviewers access the Asset and Finding Maintenance screen, the Navigation pane displays a white Visits folder. Expand this Visits folder to display its subfolders. Each subfolder represents an individual visit in VMS that has been assigned for review. Click (+) to expand the visit and display the location summaries for the visit. Within the location, DNS assets are tracked using one of the following asset types.

- Computing – Assets which have an OS such as a DNS server or appliance type device.
- Non-Computing – Used for registering DNS policy checks which are overall process and procedure checks as well as architectural requirements for the DNS infrastructure as a whole.

Assets are also listed according to the following categories.

Must Review – Assets that must be reviewed (also marked with a red exclamation point).

Reviewed – Site assets modified by the Reviewer

Not Selected for Review – Other site assets that were not targeted for review

**NOTE:** If you save changes to assets or findings in the Must Review area, VMS will automatically flag those assets as reviewed and move them to the Reviewed area.

The asset icon color in the Navigation pane indicates the severity of an open finding for the asset. The cubes on the right describe what each of the colors signifies.

- Red – CAT I
- Orange CAT II
- Yellow – CAT III
- Dark Green – No open or not reviewed items.

### 1.3.1.1 Creating Non-Computing DNS Policy Assets

To create a DNS Policy **Non-Computing** asset, perform the following steps.

1. Expand Asset Findings Maintenance.
2. Click Assets/Findings.
3. Reviewer Only: Expand Visits and skip to Step 5.
4. SA only: Expand Location then the required organization. Then skip to Step 7.
5. Reviewer Only: Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review. If the Visit is not visible, you have not been designated at the visit level as a reviewer. See your Team Lead.
6. Reviewer Only: Expand the visit and display the location summaries for the visit.
7. Click the Create icon located next to Non-Computing. The asset form is displayed.
8. Click the General tab and enter information into all required fields
  - Host Name – This must be unique for the site (e.g. DISA HQ DNS Policy)
  - Managed By – use for remote locations being managed.
  - Owner Field – use to register asset to parent or child location.
  - Mac level, Confidentiality, and Use – change or verify default values as required.

**NOTE:** The Asset Identification tab is not used for Non-Computing assets.

9. Click the Asset Posture tab to add functions to the asset.
  - Expand Non-Computing then click on DNS Policy under Directory Services.
  - Click the >> button to the selected option(s) to the Selected window
  - Click Save

### 1.3.1.2 Creating Computing DNS Assets

To create a DNS Computing asset, perform the following steps.

1. Expand Asset Findings Maintenance.
2. Click Assets/Findings.
3. Reviewer Only: Expand Visits and skip to Step 5.
4. SA only: Expand Location then the required organization. Then skip to Step 7.
5. Reviewer Only: Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review. If the Visit is not visible, you have not been designated at the visit level as a reviewer. See your Team Lead.
6. Reviewer Only: Expand the visit and display the location summaries for the visit.
7. Click the Create icon located next to Computing. The asset form is displayed.
8. Click the General tab and enter information into all required fields

- Host Name
  - Managed By – use for remote locations being managed.
  - Owner Field – use to register asset to parent or child location.
  - Mac level, Confidentiality, and Use – change or verify default values as required.
  - Status – select Online or Offline
9. Click the Asset Identification tab
- Enter IP address and click Add
  - Enter the MAC address and then click Add
10. Click the Asset Posture tab. In the Available pane, expand Computing and drill down to select the following functions:
- Operating System – drill down to required selection
  - Role – drill down to required selection
  - Application, DNS Applications, select the DNS application type (i.e. BIND, Windows DNS, CISCO CSS DNS)
  - Click the >> button to the selected option(s) to the Selected window
  - Click Save

### **1.3.1.3 Asset Finding Maintenance**

As part of the DNS review process, Reviewers enter findings manually into VMS as follows.

1. Expand Asset Findings Maintenance.
2. Expand Assets/Findings
3. Expand Visits to display its sub-folders. (*Reviewer Only SA will expand Location and proceed to step 6.*)
4. Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.
5. Expand the visit and display the location summaries for the visit.
6. Expand either Computing or Non-Computing depending on the asset type registration.
7. Expand Must Review (*Reviewer Only. SA will not see 'Must Review', but will proceed to step*
8. Expand Asset to Review. Ready to review is colored in RED
9. Expand the asset and then each Vulnerability Key.
10. Update the 'Status' of the vulnerability
11. Identify details on all open vulnerabilities
12. If applicable: Apply the same Status and comments to other assets by using the 'apply to other Findings' pane.

### **1.3.1.4 Verify All Required Assets are Updated**

1. Asset Findings Maintenance
2. Visits
3. Expand visit
4. Expand CCSD
5. Expand location
6. Expand computing or non-computing as applicable.
7. Expand Must Review. Verify checkmarks are gone from all vulnerabilities, indicating the asset is updated/reviewed.



8. If checkmarks remain from previous step, update findings using the procedures for Updating SRR Findings to VMS procedures given in a previous subsection.

### **1.3.2 Printing Compliance and Summary Reports**

Compliance and summary reports can be helpful in preparing for an SRR or for SAs in tracking and monitoring findings status.

#### **1.3.2.1 VC06 Asset Compliance Report**

1. Navigate to the Reports Menu and select the VC06 report.
2. Select to do the report by asset or an by organization as needed
3. Select “open” status
4. Sort on desired fields as required
5. Select the following to Display
  - Finding Comments
  - Finding Long Name
  - Because it’s truncated otherwise
  - Finding Details
  - Vulnerability Discussion

#### **1.3.2.2 VC03 Severity Summary Report**

Same steps as above but the report will give only the vulnerability numbers, which match the criteria selected. These reports can provide a quick check of status.

#### **1.3.2.3 AS01 Report**

The AS01 report assists the reviewer or SA by quickly identifying the assets at the location the review is being performed. In the section “Looking at Network Assets” is a quick step by step instruction in creating the report. The site may want to do other reports, if your site manages or owns assets, which are not located at the site. Check Child Locations if applicable. Navigate to the Reports menu, Select the AS01 Report, and select the desired criteria for the report.

#### **1.3.2.4 VL03 Report**

The VL03 report assists the reviewer or SA by quickly identifying the IAVMs that will be identified to the asset when you select the operating system of the asset. Navigate to the Reports menu, Select the VL03 Report, and select the desired criteria for the report.

## 2. DNS POLICY CHECKS – APPLIES TO ALL DNS ARCHITECTURES

The following checks apply to the non-computing vulnerabilities tied to DNS architectures.



**Vulnerability Key:** V0013032

**STIG ID:** DNS0100

**Vulnerability:** A name server is not protected by equivalent or better physical access controls than the clients it supports.

**IA Controls:** PEPF-1 Physical Protection of Facilities  
PEPF-2 Physical Protection of Facilities

**Categories:** 4.6 DNS

**Responsibility:** Information Assurance Officer

**References:** DNS STIG

**Severity:** Category II

### **Vulnerability Discussion:**

If an adversary can compromise a name server, then the adversary can redirect most network traffic sent to the hosts defined on that name server. Therefore, the security of the name server is as critical as the security of the hosts it protects. It is understood that different hosts require different levels of physical security. Nevertheless, the name server should not have weaker physical access controls than the computers it supports because this would, in effect, reduce the security of those hosts as well.

### **Check:** DNS0100

Ask to see the locations at the facility where computers supported by the listed name server(s) under evaluation are located (e.g., server closets, raised floor space, etc.). Note those areas that have the most extensive physical security controls. Also ask to see the locations of the name servers themselves. Then compare the physical security of the most secure computers against the physical security of the name server under evaluation. If the name server has substantially weaker physical security controls than the hosts it supports (e.g., the name server is in the DNS administrator's cube while the servers are in a locked cage in a secure raised floor area), then this is a finding.

### **Fix:** DNS0100

Working with appropriate technology and facility personnel, the IAO should arrange to relocate the name server into the same physical location as the most sensitive hosts it supports.

**OPEN:** ☐

**NOT  
APPLICABLE:** ☐

**FIXED:** ☐

**NOT A  
FINDING:** ☐

Comments:

<b>Vulnerability Key:</b>	V0013034
<b>STIG ID:</b>	DNS0110
<b>Vulnerability:</b>	The DNS log archival requirements do not meet or exceed the log archival requirements of the operating system on which the DNS software resides.
<b>IA Controls:</b>	ECRR-1 Audit Record Retention
<b>Categories:</b>	10.2 Content Configuration
<b>Responsibility:</b>	Information Assurance Officer
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category II

**Vulnerability Discussion:**

Name servers are dedicated to the DNS function and, as a result, the most critical security and operations events on those name servers will appear in the DNS logs. Different sites may have different policies regarding archival, but the DNS logs should be maintained in an equivalent (or better) manner as the operating system logs. Therefore, if operating system logs are stored for a year, then DNS logs should be stored for at least a year. If operating system logs are written to read-only media, then the DNS logs should be written to read-only media as well.

**Check:** DNS0110

This check is only applicable if DNS logs are independent from system logs. If the log archival scheme for the DNS logs is weaker than the one for the system logs, then this is a finding.

*Windows*

DNS log files are normally kept in two locations. The system event logs which can be viewed from Event Viewer found under the Administrative tools from the Start Menu. In addition, debug logging options such as query, notify, and update requirements can be viewed in a file named %systemroot%\system32\dns\dns.log.

*BIND*

BIND logging files can be found by viewing the /etc/named.conf file. Within the named.conf will be an option for logging that will display the file path to the log files. In addition, most Unix machines will also log information in the syslog on the system.

**Fix: DNS0110**

Working with appropriate technical and facility personnel, the IAO should implement an archival strategy that is at least as extensive as the current archival operation for operating system logs.

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

---

**Vulnerability Key:** V0013035

**STIG ID:** DNS0115

**Vulnerability:** DNS logs are not reviewed daily or a real-time log analysis or network management tool is not employed to immediately alert an administrator of critical DNS system messages.

**IA Controls:** ECAT-1 Audit Trail, Monitoring, Analysis and Reporting  
ECAT-2 Audit Trail, Monitoring, Analysis and Reporting

**Categories:** 10.3 Review

**Responsibility:** Information Assurance Officer

**References:** DNS STIG

**Severity:** Category II

**Vulnerability Discussion:**

If a responsible administrator does not review DNS logs daily, then there is the potential that an attack or other security issue can go unnoticed for a day or more, which is unacceptable in DoD environments.

**Check: DNS0115**

If reviewing of logs is anything less than daily, then this is a finding. In many cases, DNS logs are included within the system logs. If this is the case, then daily review of the system logs meets the requirement. If the site employs special software to scan logs for special events or key words, then this is also acceptable so long as the system issues real time alerts or is monitored at least daily.

## *Windows*

DNS log files are normally kept in two locations. The system event logs which can be viewed from Event Viewer found under the Administrative tools from the Start Menu. In addition, debug logging options such as query, notify, and update requirements can be viewed in a file named %systemroot%\system32\dns\dns.log.

## *BIND*

BIND logging files can be found by viewing the /etc/named.conf file. Within the named.conf will be an option for logging that will display the file path to the log files. In addition, most Unix machines will also log information in the syslog on the system.

### **Fix:** DNS0115

DNS software administrators should commit to reviewing logs daily, perhaps establishing a rotation for this purpose to ensure that days are not missed. Having a primary administrator and backup administrators rotate this responsibility will prevent a problem or warning sign from being missed because of an error in judgment.

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

**Vulnerability Key:** V0013036

**STIG ID:** DNS0120

**Vulnerability:** A list of personnel authorized to administer each zone and name server is not maintained.

**IA Controls:** ECPA-1 Privileged Account Control

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:**

If an organization does not document who is responsible for the DNS function, then there is a significant potential that unauthorized individuals will obtain privileged access to name servers. During a security breach, it will be difficult to assign accountability for improper transactions if it is not known who is responsible for this function.

**Check:** DNS0120

If the site POC cannot produce a list of personnel authorized to administer each zone and name server, then this is a finding.

**Fix:** DNS0120

The IAO must create and maintain a list of authorized DNS administrators for each zone and name server under the IAOs scope of responsibility.

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:

**Vulnerability Key:** V0013314

**STIG ID:** DNS0125

**Vulnerability:** A zone or name server does not have a backup administrator.

**IA Controls:** ECCD-1 Changes to Data  
ECCD-2 Changes to Data

**Categories:** 4.6 DNS

**Responsibility:** Information Assurance Officer

**Reference:** DNS STIG

**Severity:** Category II

**Vulnerability Discussion:**

If there is no backup DNS administrator, then there is nobody to assist during a security emergency when the primary administrator is unavailable. In some cases, a backup administrator can also detect problems introduced by the first administrator before these problems are allowed to propagate. Personnel redundancy is as important as technology redundancy for the DNS availability.

**Check:**

DNS0125 (Manual)

If the site POC cannot produce a list of backup personnel authorized to administer each zone and name server, then this is a finding. If any zone or name server has only one DNS database administrator or only one DNS software administrator, then this is a finding. If there is not a backup administrator for both roles, then this is a finding.

**Fixes**

DNS0125 (Manual)

Working with appropriate resource managers, the IAO should identify a backup DNS administrator for each zone and name server under the IAOs scope of responsibility.

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:



**Vulnerability Key:** V0013037

**STIG ID:** DNS0130

**Vulnerability:** A patch and DNS software upgrade log; to include the identity of the administrator, date and time each patch or upgrade was implemented, is not maintained.

**IA Controls:** ECAR-1 Audit Record Content - Public Systems  
ECAR-2 Audit Record Content - Sensitive Systems  
ECAR-3 Audit Record Content - Classified Systems

**Categories:** 10.1 Procedures

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:**

DNS software has a history of vulnerabilities and new ones may be discovered at any time. To ensure that attackers cannot take advantage of known DNS vulnerabilities, applicable software patches must be applied. Patch and DNS software upgrade documentation must be maintained to ensure the DNS name servers are protected from these vulnerabilities and current with required patches and software upgrades.

**Check:** DNS0130

DNS patch and upgrade change records must include records of the date and time each patch or upgrade to DNS software was implemented, and by whom. The method of verification may be considered weak, but the requirement is merely to document the dates and times of DNS software patch and upgrades.

**Instruction:** If there is no patch and upgrade log, then this is a finding. If there is such a log, then entries must include the date and time of any change as well as the identity of the administrator. Failure to include this information for any entry is a finding.

**Fix:** DNS0130

The SA should establish and maintain a log of the date and time each patch and upgrade to DNS software was implemented.

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

**Comments:**

<b>Vulnerability Key:</b>	V0013038
<b>STIG ID:</b>	DNS0135
<b>Vulnerability:</b>	Operating procedures do not require that DNS configuration, keys, zones, and resource record data are backed up on any day on which there are changes.
<b>IA Controls:</b>	CODB-2 Data Backup Procedures-Daily
<b>Categories:</b>	13.4 Backup & Recovery
<b>Responsibility:</b>	Information Assurance Officer
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category II

**Vulnerability Discussion:**

If a name server's configuration, keys, zones, and resource record information are not backed up on any day in which there are changes, there is a risk that an organization cannot quickly recover from the loss of the server. In addition, forensic analysis of security incidents is considerably more difficult if there is not reliable evidence of when changes may have occurred.

**Check:** DNS0135

Fortunately, by design, the DNS architecture provides built-in redundancy support. There should always be a hot backup of zone information present whenever the primary name server is unavailable for any reason (i.e., the authoritative slave server maintains a copy of the zone files on the master). This built-in redundancy, however, does not extend to configuration files and logs. Therefore, name servers should be backed up to an external media (e.g., tape, optical disk, etc.) on a regular basis.

At some locations, an automated enterprise backup system supports many servers. In this case, name servers can simply be added to the enterprise system. At other locations, backups must be performed manually, placing a considerably higher burden on administrators. In circumstances in which zone and configuration information is very static, remaining the same for several months at a time, it would make little sense to conduct daily full backups. Backups should occur as frequently as needed to capture changes on the name server.

If there are no written procedures for the backup of name servers, then this is a finding. Backup in this context refers to copying the name server's DNS configuration, keys, zones, and resource record data, at a minimum, in case it is needed for recovery at a later time. A full file system backup of the name server is preferred.

If there are written backup procedures, then it must call for the backup of DNS configuration, keys, zones, and resource record data on any day in which they were modified, if this is not the case, then this is a finding.

Any traditional daily tape backup scheme – whether it involves a full, incremental or differential scheme – will satisfy the requirement. Less frequent backups will also suffice if the configuration and resource record data are backed up whenever they are modified.

**Fix:** DNS0135

The IAO will establish operating procedures that will ensure that, at a minimum, DNS configuration, keys, zones, and resource record data is backed up on any day on which there are changes.

<b>OPEN:</b>	<input type="checkbox"/>	<b>NOT APPLICABLE:</b>	<input type="checkbox"/>	<b>FIXED:</b>	<input type="checkbox"/>	<b>NOT A FINDING:</b>	<input type="checkbox"/>
--------------	--------------------------	----------------------------	--------------------------	---------------	--------------------------	---------------------------	--------------------------

Comments:

**Vulnerability Key:** V0013039

**STIG ID:** DNS0140

**Vulnerability:** Configuration change logs and justification for changes are not maintained.

**IA Controls:** ECCD-2 Changes to Data – Access Control Mechanisms

**Categories:** 12.9 Documentation

**Responsibility:** Information Assurance Officer

**References:** DNS STIG

**Severity:** Category II

**Vulnerability Discussion:**

If changes are made to the configuration without documentation, it is often difficult to determine the root cause of an operational problem or understand the circumstances in which a security breach occurred. Without adequate configuration change records, it is also more difficult for the IAO and other oversight personnel to track major activity, which is critical to information assurance.

**Check:** DNS0140

The DNS configuration change log must note the date and time any DNS configuration files were modified and the business justification for that modification. Unless the business justification is routinely so vague as to be meaningless (e.g., “user request” for every entry), the reviewer should not second-guess what constitutes an acceptable business rationale.

Instruction: If there is no configuration change log, then this is a finding. If there are such records, then entries must include the date and time of any change and the business rationale for the change. Failure to include this information for any entry is a finding.

**Fix:** DNS0140

The IAO should implement, maintain, and periodically check compliance with configuration management requirements. The configuration change log should include, at a minimum, the date and time of any modifications to the DNS configuration files and the business justification for that modification.

**OPEN:**

☐

**NOT  
APPLICABLE:**

☐

**FIXED:**

☐

**NOT A  
FINDING:**

☐

Comments:

<b>Vulnerability Key:</b>	V0013040
<b>STIG ID:</b>	DNS0145
<b>Vulnerability:</b>	Written procedures for the replacement of cryptographic keys used to secure DNS transactions do not exist.
<b>IA Controls:</b>	ECSC-1 Security Configuration Compliance
<b>Categories:</b>	8.4 Key Management
<b>Responsibility:</b>	Information Assurance Officer
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category II

**Vulnerability Discussion:**

Without adequate cryptographic key supersession procedures, there is the potential that an unauthorized person may be able to compromise the key. Once in possession of the key, that individual might be able to update DNS records by configuring a machine to masquerade as a zone partner. Since name servers are configured to accept updates signed by a valid key, there may be no other administrative or technical controls to prevent this type of security breach.

**Check:** DNS0145

*Windows*

This check should be marked not applicable for all windows servers. Windows utilizes Active Directory for it's key management or no keys at all.

*BIND*

Like user account passwords, cryptographic keys such as TSIG keys must be changed periodically to minimize the probability that they will be compromised. If there is a known compromise of a TSIG key, then it needs to be replaced immediately. One of the most important aspects of key supersession is the method that will be used to transfer newly generated keys. Possibilities, in rough order of preference, are as follows:

- SSH
- Encrypted e-mail using DoD PKI certificates
- Secure fax (STU-III)
- Regular mail (using the expedited mailing service holding the current GSA contract for "small package overnight delivery service")

- Hand courier

Instruction: If there are no procedures for TSIG key supersession, then this is a finding. If there are such procedures, then it must cover the following:

- Frequency of key supersession
- Criteria for triggering emergency supersession events
- Notification of relevant personnel during emergency and non-emergency supersession
- Methods for securely transferring newly generated keys

This is a finding if any of these elements are missing from the supersession procedures.

**Fix:** DNS0145

The IAO should establish standard operating procedures for TSIG key supersession. These procedures should include, at a minimum, frequency of key supersession, criteria for triggering emergency supersession events, notification of relevant personnel during emergency and non-emergency supersession, and methods for securely transferring newly generated keys.

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

**Vulnerability Key:** V0013041

**STIG ID:** DNS0150

**Vulnerability:** The IAO has not established written procedures for the process of updating zone records, who is authorized to submit and approve update requests, how the DNS administrator verifies the identity of the person from whom he/she received the request, and how the DNS administrator documents any changes made.

**IA Controls:** ECCD-1 Changes to Data – Access Control Mechanisms

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer

**References:** DNS STIG

**Severity:** Category II

**Vulnerability Discussion:**

If the procedures for updating zone records are inadequate, then this increases the probability that an adversary perhaps even an insider will be able to modify the DNS records using weaknesses in administrative processes rather than weaknesses in technical controls.

**Check:** DNS0150

To best assure the integrity of zone files, one must not only carefully manage the manner in which requests are processed but also periodically check that the current records are valid. For example, when equipment is retired, people often fail to remove the associated host from the DNS. Without periodic checks, an attacker may use a retired host IP address to obtain valuable information from another user who was unaware of the change.

Instruction: If there are no written procedures for manual updates of zone files (e.g., a new host entry), then this is a finding. If there are such procedures, then it must cover the following:

- The process for updating zone records
- Who is authorized to submit and approve update requests
- How the DNS database administrator verifies the identity of the person from whom he or she received the request
- How the DNS database administrator documents any changes made

This is a finding if any of these elements are missing from the procedures for manually updating zone records.

**Fix:** DNS0150

The IAO should establish standard operating procedures for updating zone records. These procedures should include, at a minimum, the process for updating zone records, who is authorized to submit and approve update requests, how the DNS database administrator verifies the identity of the person from whom he or she received the request, and how the DNS database administrator documents any changes made.

**OPEN:** ☐ **NOT** ☐  
**APPLICABLE:** ☐ **FIXED:** ☐ **NOT A** ☐  
**FINDING:** ☐

Comments:



**Vulnerability Key:** V0013050

**STIG ID:** DNS0160

**Vulnerability:** The DNS architecture is not documented to include specific roles for each DNS server, the security controls in place, and what networks are able to query each server.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 4.6 DNS; 12.9 Documentation

**Responsibility:** Information Assurance Officer

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:**

Without current and accurate documentation, any changes to the network infrastructure may jeopardize the network's integrity. To assist in the management, auditing, and security of the network, facility drawings and topology maps are a necessity; and those addressing critical network assets, such as the DNS server, are especially important. Topology maps (documentation) are important because they show the overall layout of the network infrastructure and where devices are physically located. They also show the relationship and inter-connectivity between devices and where possible intrusive attacks (wire taps) could take place. Additionally, documentation along with diagrams of the network topology are required to be submitted to the Connection Approval Process (CAP) for approval to connect to the NIPRNet or SIPRNet. Depending on the command, service, or activity, additional approval may be required.

**Check:** DNS0160

Interview the IAO or SA and ask to see the DNS architecture documentation to include roles for each server, security controls, and the list of networks that are able to query the DNS server.

**Fix:** DNS0160

Document the DNS architecture to include the location, function, role, and security controls for all DNS servers.

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:

**Vulnerability Key:** V0013313

**STIG ID:** DNS0170

**Vulnerability:** The underlying operating system of the DNS server is not in compliance with the appropriate OS STIG.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category II

**Vulnerability Discussion:**

A vulnerability in the underlying operating system of a DNS server could potentially impact not only the DNS server but the entire network infrastructure to include the Global Information Grid (GIG).

**Checks:** DNS0170

Review the Operating System against the appropriate OS STIG. For a Windows system this would mean an evaluation with the Gold Disk; for a UNIX/LINUX system this would mean an evaluation using the SRR scripts. STIG compliance means that all findings are either closed, or there is a POA&M to address any outstanding vulnerabilities.

**Fixes:** DNS0170

The underlying Operating System of the DNS server must be in compliance with the appropriate OS STIG.

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:

**Vulnerability Key:** V0013051

**STIG ID:** DNS0175

**Vulnerability:** The DNS server software is either installed on or enabled on an operating system that is no longer supported by the vendor.

**IA Controls:** VIVM-1 Vulnerability Management

**Categories:** 12.8 Unsupported Vendor Products

**Responsibility:** Information Assurance Officer

**References:** DNS STIG

**Severity:** Category I

**Vulnerability Discussion:**

**Check:** DNS0175

Review the Operating System to determine if it is supported by the vendor, e.g. Windows NT is no longer supported.

**Fix:** DNS0175

The IAO should develop a migration plan to upgrade or replace any out of date software or any software that is no longer vendor supported.

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:

**Vulnerability Key:** V0013053

**STIG ID:** DNS0185

**Vulnerability:** The contents of zones are not reviewed at least annually.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 4.6 DNS

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:**

DNS administrators must review the contents of their zones at least annually for content or aggregation of content that may provide an adversary information that can potentially compromise operational security. This specifically includes names that provide an outsider some indication as to the function of the referenced system unless the function is obvious in the context of other standard DNS information (e.g., naming a DNS server as dns.zone.mil or an SMTP mail server as mail.zone.mil is not an OPSEC violation given that the functions of these servers are easily identifiable during DNS queries). The DNS administrator is the final adjudicator of the sensitivity of DNS information, in concert with the OPSEC processes of the organization, but should make a conscious decision to include such information based on operational need. NIST guidance includes specific guidelines that HINFO, RP and LOC records not be included in the zone.

**Check:** DNS0185

Interview the DNS administrator and ask if there is a procedure in place to review and validate the contents of the zones he/she is responsible for, at least annually.

**Fix:** DNS0185

The IAO will ensure the DNS administrator reviews the contents of the zones they are responsible for, at least annually.

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:

**Vulnerability Key:** V0013052

**STIG ID:** DNS0190

**Vulnerability:** The SA has not subscribed to ISC's mailing list "bind announce" for updates on vulnerabilities and software notifications.

**IA Controls:** VIVM-1 Vulnerability Management

**Categories:** 3.1 Security Patches

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:**

Whether running the latest version of software or an earlier version, the administrator should be aware of the vulnerabilities, exploits, security fixes, and patches for the version that is in operation in the enterprise.

**Check:** DNS0190

*Note:* This check only applies to Windows and Unix systems running BIND. It should be marked Not Applicable for those not running BIND.

If the site is using BIND, interview the SA to determine if they have subscribed to ISC's mailing list called "bind-announce" (information on the Internet at <http://www.isc.org/sw/bind/bind-lists.php>) for vulnerabilities and software notifications.

**Fix:** DNS0190

If BIND is utilized, the SA will subscribe to ISC's mailing list called "bind-announce" (information on the Internet at <http://www.isc.org/sw/bind/bind-lists.php>) for vulnerabilities and software notifications.

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:

**Vulnerability Key:** V0013042

**STIG ID:** DNS0200

**Vulnerability:** An authoritative master name server does not have at least one and preferably two or more active slave servers for each of its zones. The slave server does not reside on a separate host.

**IA Controls:** CODB-2 Data Backup Procedures Daily  
CODB-3 Data Backup Procedures Continuous

**Categories:** 4.6 DNS

**Responsibility:** Information Assurance Officer

**References:** DNS STIG

**Severity:** Category I

**Vulnerability Discussion:**

A critical component of securing an information system is ensuring its availability. The best way to ensure availability is to eliminate any single point of failure in the system itself and in the network architecture that supports it. Fortunately, the inherent design of DNS supports a high-availability environment. Master and slave servers regularly communicate zone information, so if any name server is disabled at any time, another can immediately provide the same service. The task for the network architect is to ensure that a disaster or outage cannot simultaneously impact both the master and all of its slave servers. If a disaster occurs, the DNS protocols cannot prevent total loss of name resolution services for hosts within affected zones.

**Check:** DNS0200

Using the name server configuration files, identify any zone that does not have a slave. An authoritative server for each zone must have a slave name server. If this is not the case, then this is a finding. If the slave server does not reside on a separate host, this is a finding.

*Windows (with Active Directory)*

For servers integrated with Active Directory, verify there are other domain controllers that can take over as Domain naming operations master. Open the Active Users and Computer snap in console under the Administrative tools menu. Expand the active directory domain and then expand the domain controllers folder. Ensure there are multiple domain controllers available within the domain.

*BIND*

Examine each zone file and check the NS records. There should be multiple records for the same domain with different servers authoritative for the zone. The path to the zone file can be found by examining the named.conf.

**Fix:** DNS0200

The IAO must work with appropriate personnel to obtain and configure another name server to act as a slave to the server hosting this zone.

<b>OPEN:</b>	<input type="checkbox"/>	<b>NOT APPLICABLE:</b>	<input type="checkbox"/>	<b>FIXED:</b>	<input type="checkbox"/>	<b>NOT A FINDING:</b>	<input type="checkbox"/>
--------------	--------------------------	----------------------------	--------------------------	---------------	--------------------------	---------------------------	--------------------------

Comments:

**Vulnerability Key:** V0013043

**STIG ID:** DNS0205

**Vulnerability:** Name servers authoritative for a zone are not located on separate network segments if the servers described in the zone are themselves located across more than one network segment.

**IA Controls:** CODB-3 Data Backup Procedures Continuous  
CODB-2 Data Backup Procedures Daily

**Categories:** 13.5 Redundancy

**Responsibility:** Information Assurance Officer

**References:** DNS STIG

**Severity:** Category I

**Vulnerability Discussion:**

A critical component of securing an information system is ensuring its availability. The best way to ensure availability is to eliminate any single point of failure in the system itself and in the network architecture that supports it. Fortunately, the inherent design of DNS supports a high-availability environment. Master and slave servers regularly communicate zone information, so if any name server is disabled at any time, another can immediately provide the same service. The task for the network architect is to ensure that a disaster or outage cannot simultaneously impact both the master and all of its slave servers. If a disaster occurs, the DNS protocols cannot prevent total loss of name resolution services for hosts within affected zones. The solution is to disperse name servers in such a way as to avoid single points of failure. At minimum, authoritative name servers for the same zone should be on different network segments in order that at least one name server is available in the event that a router or switch fails. This fault tolerance should also extend to wide area data communications lines. For example, if a site has multiple leased lines connecting the network on which the name server resides to a larger network such as the NIPRNet, routing protocols should be configured such that if one of the lines fails, another one will still be available to support the name server.

**Check:** DNS0205

Determine whether all the name servers supporting the same zone reside on the same subnet. If they are, this is a finding.

The reviewer can manually check the IP addresses of the servers being reviewed to determine if they are on the same subnet.

**Fix:** DNS0205



Working with appropriate technology and facility personnel, the IAO should arrange to relocate one of the name servers so that it resides on a different network segment than any other name server that hosts one or more of the same zones. In cases where the zones are small and not subject to frequent change, consideration should be given to the use of hosts or lmhost files to resolve host names.

**OPEN:** ☐      **NOT APPLICABLE:** ☐      **FIXED:** ☐      **NOT A FINDING:** ☐

Comments:

**Vulnerability Key:** V0013044

**STIG ID:** DNS0210

**Vulnerability:** A zone includes hosts located in more than one building or site, yet at least one of the authoritative name servers supporting the zone is not as geographically and topologically distributed as the most remote host.

**IA Controls:** COAS-1 Alternate Site Designation  
COAS-2 Alternate Site Designation

**Categories:** 13.5 Redundancy

**Responsibility:** Information Assurance Officer

**References:** DNS STIG

**Severity:** Category II

**Vulnerability Discussion:**

When authoritative name servers are co-located in the same facility, the loss of the facility likely leads to the loss of access to all servers defined in their zones (i.e., nobody can resolve their names). If one or more of the hosts in the supported zones are located at a different site, they would be effectively down even though they would otherwise be fully operational. This scenario can only be prevented with geographic dispersal of name servers.

**Check:** DNS0210

By examining the zone file, the reviewer can determine whether there are hosts defined on one of the name server's zones that reside in more than one building. If they all reside in the same building, then this check does not apply. If the defined hosts reside in different buildings, then one of the evaluated name server's zone partners (slave or master) must reside in an alternate building. In this case, if all of the authoritative name servers for a zone reside in the same building, then this a finding.

**Fix:** DNS0210

Working with DNS administrators and appropriate technical and facility personnel, the IAO should either arrange for one of the existing name servers to be moved to a different location, deploy an additional name server at another location, or arrange to have an existing name server at another location act as slave to the zones hosted at the current location.

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:

**Vulnerability Key:** V0013045

**STIG ID:** DNS0215

**Vulnerability:** Private IP space is used within an Enclave without the use of split DNS to prevent private IPs from leaking into the public DNS system.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 4.6 DNS

**Responsibility:** Information Assurance Officer

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:**

DNS operators should assume that any data placed in the DNS would be available to anyone connected to the Internet. Split DNS shall not be considered a mitigating factor or technique to deny DNS information to an attacker. Split DNS will continue to be required in one situation only: to prevent address space that is private (e.g., 10.0.0.0/24) or is otherwise concealed by some form of Network Address Translation from leaking into the public DNS system.

**Check:** DNS0215

This check is only applicable if the site is using private IP space within the Enclave. This is typically encountered when a site is using Network Address Translation (NAT) with private or non-routable IPs.

*BIND*

This configuration should be evidenced by the use of the view statement in the named.conf file. If it is not, then the DNS administrator must satisfactorily explain how an alternative mechanism achieves the same effect. If the site employs NAT and a split DNS configuration is not employed or a satisfactory alternative mechanism is not employed, then this is a finding. The objective is that an external DNS client should have no means of querying the DNS to obtain a host-to-IP-address mapping for an internal host that has a private or non-routable IP.

*Windows*

Review each zone and search for any private IP addresses. If private addresses are being utilized internally and their respective domain names are also capable of being accessed from outside the enclave, then ask the DNS administrator to explain if they are implementing a split DNS configuration. Note: Split DNS can also be referred to as split-horizon and split-brain DNS. The best approach is to maintain separate servers for the external/internal zone records. Most

other approaches involve forwarding from the internal server, which is against the STIG guidelines.

**Fix:** DNS0215

The IAO will ensure, when using private IP address space within an Enclave, that a split-DNS configuration is implemented to prevent the private address space from leaking into the public DNS system.

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

**Vulnerability Key:** V0013046

**STIG ID:** DNS0220

**Vulnerability:** The DNS database administrator has not documented the owner of each zone (or group of related records) and the date the zone was created, last modified, or verified. This documentation will preferably reside in the zone file itself through comments, but if this is not feasible, the DNS database administrator will maintain a separate database for this purpose.

**IA Controls:** ECCD-1 Changes to Data – Access Control Mechanisms  
ECCD-2 Changes to Data – Access Control Mechanisms

**Categories:** 4.6 DNS; 10.2 Content Configuration

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:**

A zone file should contain adequate documentation that would allow an IAO or newly assigned administrator to quickly learn the scope and structure of that zone. In particular, each record (or related set of records, such as a group of LAN workstations) should be accompanied by a notation of the date the record was created, modified, or validated and record the owner's name, title, and organizational affiliation. The owner of a record is an individual with the authority to request that the record be modified or deleted. If an organization cannot identify who is responsible for a host record, then there is no assurance that it is valid. If invalid records are in a zone, then an adversary could potentially use their existence for improper purposes.

**Check:** DNS0220

*BIND*

DNS zone record documentation will preferably reside in the zone file itself through comments, but if this is not feasible, the DNS database administrator will maintain a separate database for this purpose. The zone file location can be found by examining the named.conf and searching for the zone statement. Within the zone statement will be a file option that will display the name of the zone file.

*Windows*

Ask the DNS database administrator if they maintain a separate database with record documentation. Windows DNS does not provide the capability to insert comments for records in a zone.

Review the zone files/database. If the records are not fully documented, then this is a finding. The zone record documentation is to include, at a minimum:

- The owner of each zone record
- The date the zone record was created
- The date the zone record was last modified
- The date the zone record was last verified

Records can be grouped (e.g., a number of workstations residing in the same area or a high-availability server cluster)

**Fix:** DNS0220

The DNS database administrator will document, at a minimum, the owner of each zone record (or group of related records) and the date the record was created, last modified, or verified. This documentation will preferably reside in the zone file itself through comments, but if this is not feasible, the DNS database administrator will maintain a separate database for this purpose.

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

---

**Vulnerability Key:** V0013047

**STIG ID:** DNS0400

**Vulnerability:** The name server software on production name servers is not BIND, Windows 2000 or later DNS, or alternatives with equivalent security functionality, configured in a manner to satisfy the general security requirements listed in the STIG. The only currently approved alternative is CISCO CSS DNS.

**IA Controls:** DCPD-1 Public Domain Software Controls

**Categories:** 4.6 DNS

**Responsibility:** Information Assurance Officer

**References:** DNS STIG

**Severity:** Category II

**Vulnerability Discussion:**

If an organization runs DNS name server software other than BIND, Windows 2000 DNS or later, or an equivalent alternative, it cannot benefit from assurance testing of those implementations of DNS. As a result, there may be unknown vulnerabilities associated with the alternative products for which there are no compensating controls. Moreover, there is no detailed security implementation guidance for other name server implementations, which makes it considerably harder to conduct reviews or self assessments. An incomplete review means that an organization operates at a lower level of assurance than could have been realized with one of the approved products.

**Check:** DNS0400

Review the DNS name server software on the platform to determine what DNS software is running. If the name server is running a DNS implementation other than ISC BIND, Windows 2000/2003 or later DNS, or equivalent DNS software, then this is a finding.

The only alternative currently approved is Cisco CSS DNS, which is limited to only those hosts defined in the csd.disa.mil domain. CSS DNS is subject both to these general security requirements, where applicable, and the specific STIG guidance for this product.

**Fix:** DNS0400

Working with DNS software administrators and other appropriate technical personnel, the IAO should oversee a migration to an approved name server software.

**OPEN:**

☐

**NOT  
APPLICABLE:**

☐

**FIXED:**

☐

**NOT A  
FINDING:**

☐

Comments:

**Vulnerability Key:** V0014763

**STIG ID:** DNS0402

**Vulnerability:** The name server software on production name servers is not BIND, Windows 2000 or later DNS, or alternatives with equivalent vendor support, configured in a manner to satisfy the general security requirements listed in the STIG. The only currently approved alternative is CISCO CSS DNS.

**IA Controls:** DCPD-1 Public Domain Software Controls

**Categories:** 4.6 DNS

**Responsibility:** Information Assurance Officer

**References:** DNS STIG

**Severity:** Category I

**Vulnerability Discussion:**

If an organization runs DNS name server software other than BIND, Windows 2000 DNS or later, or an equivalent alternative, it cannot benefit from assurance testing of those implementations of DNS. As a result, there may be unknown vulnerabilities associated with the alternative products for which there are no compensating controls. Moreover, there is no detailed security implementation guidance for other name server implementations, which makes it considerably harder to conduct reviews or self assessments. An incomplete review means that an organization operates at a lower level of assurance than could have been realized with one of the approved products. Those products without vendor support can not be maintained at relevant security patch levels to assure the product has no vulnerabilities.

**Check:** DNS0402

Validation of compliance with the requirements is determined via an operating system console. An authorized SA should perform the required actions. He or she will work side-by-side with the reviewer to determine which commands are most appropriate at certain points in the review.

**UNIX**

Instruction: In the presence of the reviewer, the SA should enter the following command:

`named -v`

or,

`what /usr/sbin/named | grep named`

If a version of BIND 9.4.3-P3, BIND 9.5.1-P3 or BIND 9.6.1-P1 and above is not installed then this is a finding. If subsequent IAVA guidance recommends a BIND upgrade, then that guidance will supersede this requirement.

### Windows (With BIND)

Instruction: The reviewer must work with the SA to obtain the owner of the named.exe or dns.exe service.

In the presence of the reviewer, the SA should right-click on the named.exe or dns.exe service name file and select Properties | Version tab.

The version should be displayed in the “Description” field.

If a version of BIND prior to 9.4.3-P3 is running, then this is a finding. If subsequent IAVA guidance recommends a BIND upgrade, then that guidance will supersede this requirement.

### Windows (Native)

Instruction: The reviewer must ensure the operating system is Windows 2000 or later. If it is not, then this is a finding.

#### Fix: DNS0402

Working with DNS software administrators and other appropriate technical personnel, the IAO should oversee a migration to an approved name server software version.

OPEN:

☐

NOT  
APPLICABLE:

☐

FIXED:

☐

NOT A  
FINDING:

☐

Comments:



<b>Vulnerability Key:</b>	V0013048
<b>STIG ID:</b>	DNS0405
<b>Vulnerability:</b>	Hosts outside an enclave can directly query or request a zone transfer from a name server that resides on the internal network (i.e., not in a DMZ).
<b>IA Controls:</b>	ECAN-1 Access for Need-to-Know
<b>Categories:</b>	4.6 DNS
<b>Responsibility:</b>	Information Assurance Officer
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category II

**Vulnerability Discussion:**

If external hosts are able to query a name server on the internal network, then there is the potential that an external adversary can obtain information about internal hosts that could assist the adversary in a network attack. External hosts should never be able to learn about the internal network in this manner.

**Check:** DNS0405

Work with the Network administrator to determine whether external hosts are able to query a name server on the internal network. DNS runs on ports 53/TCP for zone transfers and 53/UDP for queries. These ports should be blocked at the firewall or router to internal DNS servers. If external hosts are able to query a name server on the internal network, then this is a finding.

**Fix:** DNS0405

Working with appropriate technical personnel, the IAO should establish firewall rules and/or router ACLs that prohibit access to the name server from external hosts.

<b>OPEN:</b>	<input type="checkbox"/>	<b>NOT</b>	<input type="checkbox"/>	<b>FIXED:</b>	<input type="checkbox"/>	<b>NOT A</b>	<input type="checkbox"/>
		<b>APPLICABLE:</b>				<b>FINDING:</b>	

Comments:

<b>Vulnerability Key:</b>	V0004027
<b>STIG ID:</b>	EN540
<b>Vulnerability:</b>	Servers do not employ Host Based Intrusion Detection (HIDS).
<b>IA Controls:</b>	ECID-1 Host Based IDS
<b>Categories:</b>	14.6 HIDS/Personal Firewalls
<b>Responsibility:</b>	System Administrator
<b>References:</b>	Enclave STIG
<b>Severity:</b>	Category II

**Vulnerability Discussion:**

Servers without a HID may allow unauthorized access to go undetected and limit the ability of security personnel to stop malicious or unauthorized use of the device. In order to ensure that an attempted or existing attack goes unnoticed, the data from the HID must be monitored continuously.

**Check:** EN540

Interview the IAO to determine if there is a process and policy in place to ensure Host Based IDS is installed on all servers.

Work with the reviewers to determine compliance.

A few applications that provide host-based network intrusion protection are:

Dragon Squire by Enterasys Networks

ITA by Symantec

Hostsentry by Psionic Software

Logcheck by Psionic Software

RealSecure agent by ISS

Swatch by Stanford University

Ask the SA or IAO if a host-based intrusion detection application is loaded on the system. Use the command:

```
# find / -name <daemon name> -print
```

(where <daemon name> is the name of the primary application daemon) to determine if the application is loaded on the system. Use the command:

```
# ps -ef | grep <daemon name>
```

to determine if the application is active on the system.

## Windows:

Review the installed applications/programs to see if a HID is employed. Check for any services that may be running for this purpose.

The reviewer should examine the Windows Services GUI to identify started services (in Windows 2000/2003, right click on “My Computer” and select “Manage.” In the left windowpane, click on “Services and Applications.” A list of services is displayed in the right windowpane.

### Fix: EN540

The IAO will ensure all servers employ HIDS, if technically feasible. This requirement may not pertain to legacy systems and cutting edge devices that do not yet have the capability. Documentation must exist from the vendor to approve any variance from this requirement.

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

### **3. ALL WINDOWS OS AND UNIX OS DNS PLATFORMS (BIND AND WINDOWS DNS)**

--

<b>Vulnerability Key:</b>	V0004467
<b>STIG ID:</b>	DNS0225
<b>Vulnerability:</b>	Record owners will validate their zones no less than annually. The DNS database administrator will remove all zone records that have not been validated in over a year.
<b>IA Controls:</b>	ECSC-1 Security Configuration Compliance
<b>Categories:</b>	4.6 DNS
<b>Responsibility:</b>	Information Assurance Officer
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category III

**Vulnerability Discussion:**

If zone information has not been validated in over a year, then there is no assurance that it is still valid. If invalid records are in a zone, then an adversary could potentially use their existence for improper purposes. An SOP detailing this process can resolve this requirement.

**Check:** DNS0225

*BIND*

DNS zone record documentation will preferably reside in the zone file itself through comments, but if this is not feasible, the DNS database administrator will maintain a separate database for this purpose. The zone file location can be found by examining the named.conf and searching for the zone statement. Within the zone statement will be a file option that will display the name of the zone file. The reviewer should check that the record's last verified date is less than one year prior to the date of the review. If this is not the case for any host or group of hosts, then this is a finding.

*Windows*

Ask the DNS database administrator if they maintain a separate database with record documentation. Windows DNS does not provide the capability to insert comments for records in a zone. The reviewer should check that the record's last verified date is less than one year prior to the date of the review. If this is not the case for any host or group of hosts, then this is a finding.

**Fix:** DNS0225

Working with DNS Administrators and other appropriate technical personnel, the IAO should attempt to validate the hosts with expired validation dates. If these cannot be validated within a reasonable period of time, they should be removed.

A zone file should contain adequate documentation that would allow an IAO or newly assigned administrator to quickly learn the scope and structure of that zone. In particular, each record (or related set of records, such as a group of LAN workstations) should be accompanied by a notation of the date the record was created, modified, or validated and record the owner's name, title, and organizational affiliation. The owner of a record is an individual with the authority to request that the record be modified or deleted.

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

---

<b>Vulnerability Key:</b>	V0004468
<b>STIG ID:</b>	DNS0230
<b>Vulnerability:</b>	Resource records for a host in a zone file are included and their fully qualified domain name should reside in another zone. The exception is a glue record or CNAME record supporting a system migration.
<b>IA Controls:</b>	ECSC-1 Security Configuration Compliance
<b>Categories:</b>	4.6 DNS
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category III

**Vulnerability Discussion:**

If a name server were able to claim authority for a resource record in a domain for which it was not authoritative, this would pose a security risk. In this environment, an adversary could use illicit control of a name server to impact IP address resolution beyond the scope of that name server (i.e., by claiming authority for records outside of that servers zones). Fortunately, all but the oldest versions of BIND and most other DNS implementations do not allow for this behavior. Nevertheless, the best way to eliminate this risk is to eliminate from the zone files any records for hosts in another zone. The two key exceptions to this rule involve glue for NS records and CNAME records for legacy resolution support

**Check:** DNS0230

Review the zone files and confirm with the DNS administrator that the hosts defined in the zone files do not reside in another zone with its fully qualified domain name. If extraneous resource records are maintained, then this is a finding.

#### *BIND*

The zone file location can be found by examining the named.conf and searching for the zone statement. Within the zone statement will be a file option that will display the name of the zone file. Review the zone file and check for records that contain domain names outside of the zone. I.E. A zone named fso.chambersburg.com will not have a record for a host with a domain ending in disa.mil.

#### *Windows*

Open the DNS management snap in for the Administrative Tools menu. Expand the Forward Lookup Zones folder. Expand each zone and ensure the name column for each record does not contain a name for a record that resides outside of the zone. I.E. A zone named fso.chambersburg.com will not have a record for a host with a domain ending in disa.mil.

#### **Fix:** DNS0230

The DNS database administrator should remove any resource records for a host in a zone file if its fully qualified domain name resides in another zone, unless the record is a glue record or temporary CNAME record supporting a system migration.

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

---

<b>Vulnerability Key:</b>	V0004469
<b>STIG ID:</b>	DNS0235
<b>Vulnerability:</b>	Zone-spanning CNAME records, that point to a zone with lesser security, are active for more than six months.
<b>IA Controls:</b>	ECSC-1 Security Configuration Compliance
<b>Categories:</b>	4.6 DNS
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category III

### Vulnerability Discussion:

The use of CNAME records for exercises, tests or zone-spanning aliases should be temporary (e.g., to facilitate a migration). When a host name is an alias for a record in another zone, an adversary has two points of attack, the zone in which the alias is defined and the zone authoritative for the aliases canonical name. This configuration also reduces the speed of client resolution because it requires a second lookup after obtaining the canonical name. Furthermore, in the case of an authoritative name server, this information is promulgated throughout the enterprise to caching servers and thus compounding the vulnerability.

**Check:** DNSS0235

#### *BIND*

The zone file location can be found by examining the named.conf and searching for the zone statement. Within the zone statement will be a file option that will display the name of the zone file. The record type column will display CNAME. This is usually the third or fourth field in a record depending if the TTL value is utilized. Without a TTL value, the CNAME type will be in the third field, otherwise it will display as the fourth field. Review the zone files and the DNS zone record documentation to confirm that there are no CNAME records older than 6 months. If there are CNAME records older than 6 months, then this is a finding.

#### *Windows*

Open the DNS management snap in for the Administrative Tools menu. Expand the Forward Lookup Zones folder. Review the type column for each record to locate those with a type of Alias (CNAME). Ask the DNS administrator to see the database with the record documentation is stored to confirm there are not CNAME records older than 6 months.

**Fix:** DNS0235

The DNS database administrator should remove any zone-spanning CNAME records that have been active for more than six months.

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

---

**Vulnerability Key:** V0004470

**STIG ID:** DNS0240



<b>Vulnerability:</b>	The DNS database administrator has not ensured each NS record in a zone file points to an active name server authoritative for the domain specified in that record.
<b>IA Controls:</b>	ECSC-1 Security Configuration Compliance
<b>Categories:</b>	4.6 DNS
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category I

**Vulnerability Discussion:**

Poorly constructed NS records pose a security risk because they create conditions under which an adversary might be able to provide the missing authoritative name services that are improperly specified in the zone file. The adversary could issue bogus responses to queries that clients would accept because they learned of the adversary's name server from a valid authoritative name server, one that need not be compromised for this attack to be successful. The list of slave servers must remain current within 72 hours of any changes to the zone architecture that would affect the list of slaves. If a slave server has been retired or is not operational but remains on the list, then an adversary might have a greater opportunity to impersonate that slave without detection, rather than if the slave were actually online. For example, the adversary may be able to spoof the retired slave's IP address without an IP address conflict, which would likely not occur if the true slave were active.

**Check:** DNS0240

*BIND*

The zone file location can be found by examining the named.conf and searching for the zone statement. Within the zone statement will be a file option that will display the name of the zone file. Review the zone files, and confirm with the DNS administrator that each NS record points to an active name server authoritative for the domain, if this is not the case, then this is a finding.

*Windows*

Open the DNS management snap in for the Administrative Tools menu. Expand the Forward Lookup Zones folder. Review the type column for each record to locate those with a type of Name Server (NS). Confirm with the DNS administrator that each NS record points to an active name server authoritative for the domain, if this is not the case, then this is a finding.

**Fix:** DNS0240

The DNS database administrator should remove any NS records in a zone file that do not point to an active name server authoritative for the domain specified in that record.

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

---

**Vulnerability Key:** V0004473

**STIG ID:** DNS0415

**Vulnerability:** DNS software does not run on dedicated (running only those services required for DNS) hardware. The only currently accepted exception of this requirement is Windows 2000/2003 DNS, which must run on a domain controller that is integrated with Active Directory services.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 4.6 DNS

**Responsibility:** Information Assurance Officer

**References:** DNS STIG

**Severity:** Category II

**Vulnerability Discussion:**

Even a securely configured operating system is vulnerable to the flaws of the programs that run on it. To prevent DNS software from being subjected to the vulnerabilities of other programs and services, the DNS server will not run other programs and services at all, or at least run only those programs that are necessary for either OS or DNS support.

**Check:** DNS0415

During the initial interviews, the reviewer may have already identified that a name server is supporting production services other than DNS. At this point, the reviewer should validate that response through a hands-on check of the actual name server.

*UNIX*

The only permitted services to be running on a DNS UNIX BIND server are those implementing:

- DNS
- Secure shell
- Host intrusion detection
- Host file integrity

- Network management or monitoring
- Anti-virus
- Backup
- UPS
- NTP

The below are not permitted:

Services started through inetd.conf:

admind, chargen, echo, etherstatd, fingerd, ftpd, httpd, ICQ server, identd, netstat, netstatd, nit, nntp, nsed, nsemttd, pfilt, portd, quaked, rexd, rexecd, rje\_mapper, rlogind, rpc\_3270, rpc\_alias, rpc\_database, rpc\_keyserv, rpc\_sched, rquotad, rsh, rstatd, rusersd, selectd, serverd, showfhd, sprayd, statmon, sunlink\_mapper, sysstat, talkd, telnetd, tfsd, tftpd, timed, ttdd, ugidd, uucpd, and walld.

Services started at boot time:

NFS client, NFS server process and SNMP daemon, automounter, printer queue daemon, and RPC portmapper. (For Solaris, disable the following scripts in rc2.d: S73nfs.client, S74autofs, S80lp, S71rpc, and S99dtlogin and the following scripts in rc3.d: S15nfs.server and S76snmpd.)

Instruction: In the presence of the reviewer, the SA should enter the following command:

ps -ef

Based on the command output, the reviewer should be able to determine if the machine is dedicated to DNS or if it is supporting other production services. If additional services are running and it is determined the name server is not running on dedicated hardware, then this is a finding.

### *Windows*

The only permitted services to be running on a ISC BIND or Windows DNS server are those implementing:

- DNS (i.e., the ISC BIND service) or
- DNS Server (i.e., Windows 2000 DNS)
- Host intrusion detection
- Host file integrity
- Network management or monitoring
- Anti-virus
- Backup
- UPS
- Active Directory/Domain Controller Services including:

Alerter Service COM+ Event System Computer Browser Distributed File System (DFS)	Network Connections NTLM Security Support Provider Plug and Play Print Spooler
---	---

DNS Client	Protected Storage
DNS Server	Remote Procedure Call (RPC)
Event Log	Remote Procedure Call (RPC) Locator
File Replication Service	Remote Registry Service
Intersite Messaging	Security Accounts Manager
IPSec Policy Agent	Server
Kerberos Key Distribution Center	System Event Notification
Logical Disk Manager	TCP/IP NetBIOS Helper Service
Logical Disk Manager Administrative Service	Windows Management Instrumentation
Messenger	Windows Management Instrumentation Driver Extensions
Net Logon	Windows Time
	Workstation

**Instruction:** The reviewer should examine the Windows Services GUI to identify started services (in Windows 2000/2003, right click on “My Computer” and select “Manage.” In the left windowpane, click on “Services and Applications.” A list of services is displayed in the right windowpane. Click on the “Status” column heading to sort by status. The started services will be grouped together). Also check the “Applications” tab of “Task Manager” for applications that do not run as a service. (Simultaneously press Ctrl-Alt-Del keys and select the “Applications” tab.)

Based on this examination, the reviewer should be able to determine if the machine is dedicated to DNS or if it is supporting other production services. If additional services are running and it is determined the name server is not running on dedicated hardware, then this is a finding. The exception is Windows 2000/2003 DNS, which may run domain controllers that host Active Directory services.

**Fix:** DNS0415

Working with DNS and Systems Administrators, the IAO should migrate the DNS software to dedicated hardware for the purpose of supporting the name server or remove/migrate any additional programs or applications, running on the name server to ensure the name server is running on dedicated hardware.

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

---

<b>Vulnerability Key:</b>	V0004475
<b>STIG ID:</b>	DNS0420
<b>Vulnerability:</b>	Permissions on files containing DNS encryption keys are inadequate.
<b>IA Controls:</b>	ECCD-1 Changes to Data ECCD-2 Changes to Data
<b>Categories:</b>	2.1 Object Permissions
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category II

**Vulnerability Discussion:**

Weak permissions could allow an intruder to view or modify DNS encryption key files. For Windows systems, this check will only apply to those running ISC BIND.

**Check:** DNS0420

*UNIX*

Instruction: The reviewer must work with the SA to obtain the user name running the named process.

In the presence of the reviewer, the SA should enter the following command to obtain the owner of the named process:

```
ps -ef | grep named
```

The location to the encryption keys can be found by examining the keys directive in the /etc/named.conf file. In the presence of the reviewer, the SA should enter the following command while in the directory containing the DNS encryption keys:

```
ls -la 'encryption_key_file'
```

If the DNS encryption key files have permissions weaker than 640, then this is a finding.

*Windows with BIND*

Instruction: The reviewer must work with the SA to obtain the owner of the named.exe. In the presence of the reviewer, the SA should right-click on the named.exe file and select Properties | Security tab | Advanced | Owner tab.

For each DNS encryption key file listed in c:\named\etc\named.conf keys directive , right-click on the file and select Properties | Security tab.

If the DNS encryption key files have permissions that allow read access to anyone beyond the owner of the named.exe, then this is a finding.

Windows DNS with Active Directory should be marked Not Applicable for this check.

**Fix:** DNS0420

The SA should modify permissions of the files containing DNS encryption keys so that only the DNS software process ID (PID) has read access to these files.

OPEN: ☐      NOT  
APPLICABLE: ☐      FIXED: ☐      NOT A  
FINDING: ☐

Comments:

<b>Vulnerability Key:</b>	V0004476
<b>STIG ID:</b>	DNS0425
<b>Vulnerability:</b>	Users and/or processes other than the DNS software account and/or the DNS database administrator have edit/write access to the zone database files.
<b>IA Controls:</b>	ECCD-1 Changes to Data ECCD-2 Changes to Data
<b>Categories:</b>	2.1 Object Permissions
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category II

**Vulnerability Discussion:**

Weak permissions on zone files could allow an intruder to view or modify DNS zone files. Permissions on these files will be 640 or more restrictive.

**Check:** DNS0425

*UNIX*

Instruction: The reviewer must work with the SA to obtain the username and groupname of the DNS database administrator, DNS software administrator, and the username running the named daemon process.

In the presence of the reviewer, the SA should enter the following command to obtain the owner of the named process:

```
ps -ef | grep named
```

There are different ways (e.g., password/group file, NIS+, etc.) to obtain the DNS database administrator's username and groupname, the reviewer is to work with the SA to obtain this information based on the configuration of the site's UNIX OS.

The zone files can be located by viewing the named.conf configuration for the zone statement and the file directive contained within the zone statement. In the presence of the reviewer, the SA should enter the following command while in the directory containing the zone files:

```
ls -l
```

If the zone files have permissions that allow write access to anyone beyond the owner of the named process or the DNS database administrator then this is a finding.

### *Windows*

**Instruction:** The review must obtain the username and groupname of the DNS database administrator. The reviewer must work with the SA to obtain the owner of the named.exe or dns.exe program.

In the presence of the reviewer, the SA should right-click on the named.exe or dns.exe file and select Properties | Security tab | Advanced | Owner tab.

For each Standard or Primary zone file, right-click on the file in %SystemRoot%\System32\Dns and select Properties | Security tab.

If the zone files have permissions that allow write access to anyone beyond Administrators, Enterprise Domain Controllers, Enterprise Admins, Domain Admins, System or DNS Admins, then this is a finding.

For Active directory integrated zones, the permissions of the Active Directory database should be verified. The usually resides in %SystemRoot%\NTDS\ntds.dit The permissions should only give full control access to System, Administrators, Creator Owner, and Local Service. Any others, then this is a finding.

### **Fix:** DNS0425

The SA should modify permissions of zone files that only the DNS software PID and/or the DNS database administrator have edit access to the zone database files.

**OPEN:** ☐      **NOT APPLICABLE:** ☐      **FIXED:** ☐      **NOT A FINDING:** ☐

Comments:

---



<b>Vulnerability Key:</b>	V0004477
<b>STIG ID:</b>	DNS0430
<b>Vulnerability:</b>	Users or processes other than the DNS software administrator and the DNS software account have read access to the DNS software configuration files and/or users other than the DNS software administrator have write access to these files.
<b>IA Controls:</b>	ECCD-1 Changes to Data ECCD-2 Changes to Data
<b>Categories:</b>	2.1 Object Permissions
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category II

**Vulnerability Discussion:**

Weak permissions on key DNS configuration files could allow an intruder to view or modify DNS name server configuration files. This check can apply to both Windows and UNIX BIND. The named.conf is a good place to start to check the permissions. View the named.conf to obtain the configuration path to the zone files. Verify the permissions of the zone files also.

**Check:** DNS0430

*UNIX*

Instruction: The reviewer must work with the SA to obtain the username and groupname of the DNS software administrator and the username running the named daemon process.

In the presence of the reviewer, the SA should enter the following command to obtain the owner of the named process:

```
ps -ef | grep named
```

There are different ways (i.e., password/group file, NIS+, etc.) to obtain the DNS software administrator's username and groupname, the reviewer is to work with the SA to obtain this information based on the configuration of the site's UNIX OS.

In the presence of the reviewer, the SA should enter the following command while in the directory containing the DNS configuration files:

```
ls -l /etc/named.conf
```

If the DNS configuration files have permissions that allow write access to anyone beyond the DNS software administrator or permissions that allow read access to anyone beyond the owner of the named process or the DNS software administrator then this is a finding.

### *Windows*

For ISC BIND:

Instruction: The reviewer must work with the SA to obtain the username and groupname of the DNS software administrator and the owner of the named.exe or dns.exe or dns.exe program.

In the presence of the reviewer, the SA should right-click on the named.exe or dns.exe file and select Properties | Security tab | Advanced | Owner tab.

The reviewer should ask the SA for the location of the ISC BIND named.conf/zone files. For each DNS configuration file, right-click on the file and select Properties | Security tab.

If the DNS configuration files have permissions that allow write access to anyone beyond the DNS software administrator or permissions that allow read access to anyone beyond the owner of the named process or the DNS software administrator then this is a finding.

For Windows DNS:

Open the DNS management console and expand the Forward Lookup Zones. Right click on each zone and select **Properties**. Select the **Security** tab. If the DNS configuration files have permissions that allow write access to anyone beyond the DNS software administrator or permissions that allow read access to anyone beyond the owner of the dns.exe process or the DNS software administrator then this is a finding.

### **Fix:** DNS0430

The SA should modify permissions of the DNS name server configuration files so that only the DNS software administrator and the DNS software PID have read access to the DNS software configuration files and that only the DNS software administrator has write access to these files.

OPEN:	<input type="checkbox"/>	NOT APPLICABLE:	<input type="checkbox"/>	FIXED:	<input type="checkbox"/>	NOT A FINDING:	<input type="checkbox"/>
-------	--------------------------	--------------------	--------------------------	--------	--------------------------	-------------------	--------------------------

Comments:

---

<b>Vulnerability Key:</b>	V0004478
<b>STIG ID:</b>	DNS0435
<b>Vulnerability:</b>	The name server's IP address is NOT statically defined and configured locally on the server. The name server has a DHCP address.
<b>IA Controls:</b>	ECSC-1 Security Configuration Compliance
<b>Categories:</b>	4.6 DNS
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category II

**Vulnerability Discussion:**

Static IP addresses permit a machine to offer Internet services like web, ftp, DNS, and email. Because a specific, known address is associated with your connection, other machines on the Internet know where to send traffic destined for your server. Required ACL restrictions at the router and or firewall are required to protect the DNS server from unauthorized access. Such ACLS require a static IP address to be effective.

**Check:** DNS0435

*UNIX*

Instruction: In the presence of the reviewer, the SA should enter the following command to verify the IP address is not obtained by DHCP, hme0 is used as an example, please confirm the interface:

```
ifconfig hme0 auto_dhcp status
```

If "Ifconfig: hme0: interface is not under DHCP control," is not displayed, then this is a finding.

Please note this above mentioned command does not work on every version of UNIX, if this command does not work, please use the below instruction.

In the presence of the reviewer, the SA enters the following command while in the /etc directory: The reviewer should ensure the file /etc/dhpc.hme0 is not located on the server.

```
ls -l
```

If the file dhcp.hme0 is listed (interface designation may different), then this is a finding.

### *Windows*

**Instruction:** In the presence of the reviewer, the SA should select Start | Run, this will bring up the “Run” dialog box. Type cmd at the command line, this will bring up the command screen. Enter the following command:

ipconfig /all

If “DHCP Enabled” is not set to “No,” then this is a finding.

**Fix:** DNS0435

The SA should configure the name server with an IP address that is statically defined.

<b>OPEN:</b>	<input type="checkbox"/>	<b>NOT APPLICABLE:</b>	<input type="checkbox"/>	<b>FIXED:</b>	<input type="checkbox"/>	<b>NOT A FINDING:</b>	<input type="checkbox"/>
--------------	--------------------------	----------------------------	--------------------------	---------------	--------------------------	---------------------------	--------------------------

Comments:

---

<b>Vulnerability Key:</b>	V0004479
<b>STIG ID:</b>	DNS0440
<b>Vulnerability:</b>	An integrity checking tool is not installed or not monitoring for modifications to the root.hints and named.conf files.
<b>IA Controls:</b>	ECSC-1 Security Configuration Compliance
<b>Categories:</b>	10.1 Procedures
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category II

**Vulnerability Discussion:**

An integrity checking tool compares file and directory integrity to the baseline. It can alert the system administrator to unauthorized changes in files or directories. Unauthorized changes in files and directories can give a user unauthorized access to system resources. Undetected changes to DNS name server root hints and configuration files is the single greatest risk to the security and stability of the DNS name server. An integrity checking tool (e.g., Tripwire) aids in effectively monitoring and controlling changes to ensure improved security and system availability. This applies to both authoritative and caching name servers.

**Check:** DNS0440

*UNIX*

Instruction: The reviewer must work with the SA to obtain the program name.

In the presence of the reviewer, the SA should enter the following command to confirm the integrity checking tool is installed and running:

```
ps -ef | grep process name
```

If an integrity checking tool is not installed and running, then this is a finding.

With the assistance of the SA, confirm that the integrity checking tool is monitoring for any modifications to the root hints and name server's configuration (e.g., named.conf), if this is not the case, then this is a finding. If using ISC BIND name server software, common names for the root hints file are root.hints, named.cache, or db.cache. The name is configurable within the named.conf file. rndc.conf will be protected in the same manner.

## Windows

**Instruction:** The reviewer must work with the SA to obtain the service name.

**Instruction:** The reviewer should examine the Windows Services GUI to identify started services (in Windows 2000/2003, right click on “My Computer” and select “Manage”. In the left windowpane, click on “Services and Applications”. A list of services is displayed in the right windowpane. Click on the “Status” column heading to sort by status. The started services will be grouped together). Also check the “Applications” tab of “Task Manager” for applications that do not run as a service (Simultaneously press Ctrl-Alt-Del keys and select the “Applications” tab). The reviewer should be able to determine if an integrity checking tool is installed and running.

If an integrity checking tool is not installed and running, then this is a finding.

With the assistance of the SA, confirm that the integrity checking tool is monitoring for any modifications to the root hints, which can be found C:/Windows/System32/DNS/cache.dns. In addition ensure the tool is checking the zone files. Although active directory zone files are stored in the active directory database, ntds.dit will not be able to be monitored with integrity checking as it is a database file and will be changing size and checksum. For non-active directory zones, obtain the name of the zone from the DNS management console list of forward zones. Enter the zone name into the windows search and it will display the path to the actual zone files, normally found in a backup directory.

### **Fix:** DNS0440

The SA should install an integrity checking tool on the name server and configure the tool to monitor for any modifications to the root.hints and name server configuration files.

**OPEN:** ☐      **NOT APPLICABLE:** ☐      **FIXED:** ☐      **NOT A FINDING:** ☐

**Comments:**

---

<b>Vulnerability Key:</b>	V0004481
<b>STIG ID:</b>	DNS0450
<b>Vulnerability:</b>	Dynamic updates are not cryptographically authenticated.
<b>IA Controls:</b>	DCNR-1 Non-repudiation – Cryptography Standard
<b>Categories:</b>	8.6 Object Integrity
<b>Responsibility:</b>	Information Assurance Officer
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category I

**Vulnerability Discussion:** The dynamic update capability has considerable appeal in an environment in which IP addresses change so frequently that it would be unacceptably burdensome or expensive to dedicate the time of a DNS database administrator to this function. This condition would likely be met at sites that rely on the Dynamic Host Configuration Protocol (DHCP) to assign IP addresses to client devices such as workstations, laptops, and IP telephones. It would also apply to sites that utilize frequently changing service (SRV) records. On the other hand, dynamic updates can pose a security risk if the proper security controls are not implemented. When dynamic updates are permitted without any mitigating controls, a host with network access to the name server can modify any zone record with an appropriately crafted dynamic update request. The solution is to require cryptographic authentication of all dynamic update requests, but not all DNS software supports this functionality.

**Check:** DNS0450

### *BIND*

**Instruction:** The reviewer should review the configuration files and check each zone statement for the presence of the allow-update phrase, which enables cryptographically authenticated dynamic updates:

The reviewer should identify the allow-update phrase. The following example disables dynamic updates:

```
allow-update {none;};
```

In addition, the absence of the allow-update clause will deny updates by default.

If dynamic updates are not disabled, as shown in the above example, they must be cryptographically authenticated as shown in the below example.

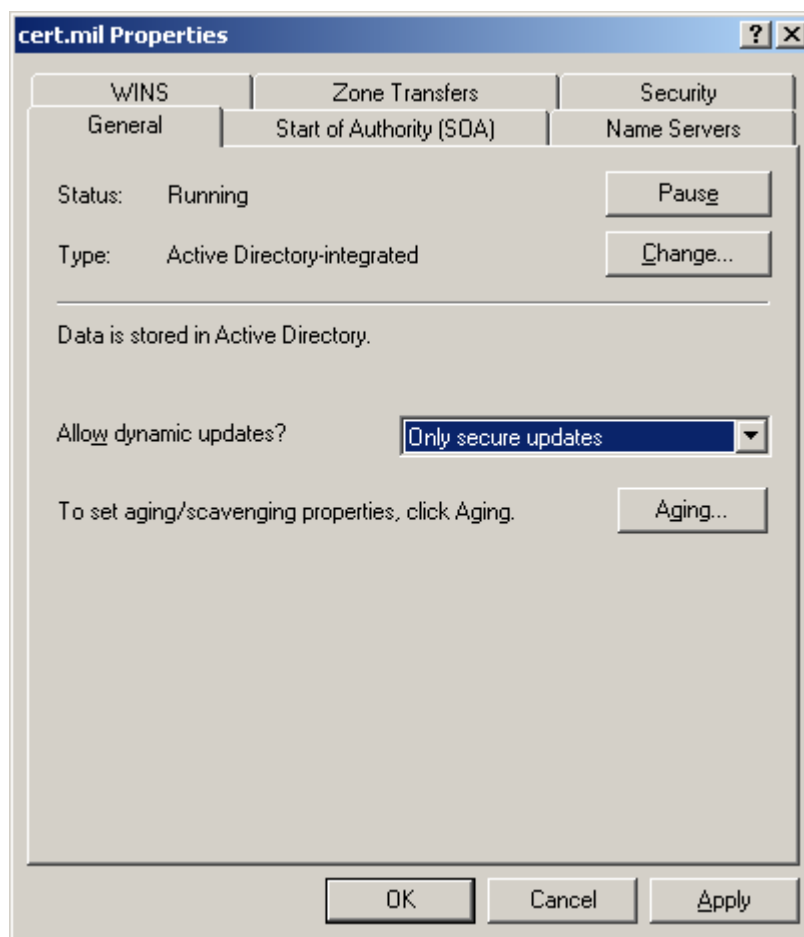
The following example demonstrates cryptographically authenticated dynamic updates:

```
allow-update {key ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil;  
};
```

If dynamic updates are not disabled or cryptographically authenticated, then this is a finding.

#### *Windows 2000/2003 DNS*

Instruction: In the presence of the reviewer, the SA must review the “Properties” dialog box, select the “General” tab, and check to see if dynamic updates are allowed. If dynamic updates are enabled, ensure that “Only secure updates” has been selected. If this is not the case, then this is a finding.



#### **Fix:** DNS0450

For BIND implementations, the DNS software administrator must ensure that each zone statement in named.conf contains the phrase `allow update{none;};` to disable dynamic updates or `allow-update {key ks1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil;};` (this is an example key name) to encrypt dynamic updates. For Windows 2000 DNS, disable dynamic updates or if dynamic updates are allowed via the General tab within the Properties dialog box, the DNS



software administrator should select Only secure updates. In cases in which the name server is not running BIND or Windows 2000 DNS, the DNS software administrator must determine how to disable dynamic updates or encrypt them. If this is not possible, then the product must be replaced as soon as it is feasible to do so.

**OPEN:** ☐      **NOT APPLICABLE:** ☐      **FIXED:** ☐      **NOT A FINDING:** ☐

Comments:

---

<b>Vulnerability Key:</b>	V0004482
<b>STIG ID:</b>	DNS0455
<b>Vulnerability:</b>	The DNS software administrator will configure each master/slave server supporting a zone to cryptographically authenticate zone transfers.
<b>IA Controls:</b>	DCNR-1 Non-repudiation – Cryptography Standard
<b>Categories:</b>	1.4 Authentication Services
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category I/II

**Vulnerability Discussion:**

A slave updates its zone information by requesting a zone transfer from its master. In this transaction, the risk for the slave is that the response to its request is not in fact from its authorized master but from an adversary posing as the master. In this scenario, such an adversary would be able to modify and insert records into the slave's zone at will. To protect against this occurrence, the slave must be able to authenticate the master to provide assurance that any zone updates are valid. For Windows DNS zones integrated with Active Directory, this check should be marked Not a Finding.

**Check:** DNS0455

*BIND*

Instruction: This check is only applicable to slave servers. If there is not an allow-transfer phrase within the zone statement, then this is a CAT I finding. If there is an allow-transfer statement, there must be a TSIG key corresponding to each of the zone partners. The reviewer can validate this by examining the key and server statements within named.conf. Check the keys phrase within each of the server statements. Verify the key statement is configured to cryptographically authenticate the master name server; an example is provided below, if this is not configured, then this is a finding.

On the master name server, this is an example of a configured key statement:

```
key ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil. {  
  algorithm hmac-md5;  
  include "/etc/dns/keys/tsig-example.key";  
};
```

```
zone "disa.mil" {  
type master;file "db.disa.mil";  
allow-transfer { key ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil.; };  
};
```

On the slave name server, this is an example of a configured key statement:

```
key ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil. {  
    algorithm hmac-,d5;  
    include "/etc/dns/keys/tsig-example.key";  
};  
  
server 10.2.2.2 {  
    keys {ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil};  
};  
  
zone "disa.mil" {  
    type slave;  
    masters { 10.1.1.1; };  
    file "db.disa.mil";  
};
```

A violation of this requirement can have one of two severity levels depending upon the extent of the violation. If slaves do not authenticate master servers in any manner, then the discrepancy would be a Category I finding. If some form of authentication exists (i.e., based on IP address), but it is not based on cryptography, then the discrepancy would be a Category II finding.

#### *Windows 2000/2003 DNS:*

**Instruction:** This check only applies if the name server is not active directory integrated. If the Windows DNS zone type is not active directory integrated, then open the DNS management console snap-in, right click on the zone and select properties. If the name servers tab has entries, then this will still be a CAT II finding. If the name servers tab does not have entries, then this is a CAT I.

In cases in which the name server is not running BIND or Windows DNS, the reviewer must still examine the configuration and its documentation to validate this requirement.

#### ***Mitigation:***

A violation of this requirement can have one of two severity levels depending upon the extent of the violation. If slaves do not authenticate masters in any manner, then the discrepancy would be a Category I finding. If some form of authentication exists (i.e., based on IP address), but it is not based on cryptography, then the discrepancy would be a Category II finding.

#### **Fix:** DNS0455

The DNS software administrator should configure each slave supporting a zone to cryptographically authenticate its master before accepting zone updates.

OPEN:

☐

NOT  
APPLICABLE:

☐

FIXED:

☐

NOT A  
FINDING:

☐

Comments:

---

**Vulnerability Key:** V0004483

**STIG ID:** DNS0460

**Vulnerability:** A zone master server does not limit zone transfers to a list of active slave name servers authoritative for that zone.

**IA Controls:** ECAN-1 Access for Need-to-Know: Discretionary Access

**Categories:** 4.6 DNS

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category II

**Vulnerability Discussion:**

The risk to the master in this situation is that it would honor a request from a host that is not an authorized slave, but rather an adversary seeking information about the zone. To protect against this possibility, the master must first have knowledge of what machines are authorized slaves.

**Check:** DNS0460

*BIND*

Instruction: This check is only applicable to zone master servers. If there are no allow-transfer phrases within named.conf, then this is a finding. If there are allow-transfer phrases, then check that there is one corresponding to each of the zone partners. If this is not the case, then this is also a finding.

If there are allow-transfer phrases for servers other than those supplied, then there may be a finding associated with the incompleteness of the list.

If the key statement references a file, then no other key statement should reference the same file.

If the key statement includes a character representation of the key itself (an improper configuration), then no other key statement should include the same character string.

On the master name server, this is an example of a configured allow-transfer phrase:

```
zone "disa.mil" {  
    type master;  
    file "db.disa.mil";  
    allow-transfer { 10.10.10.1; key ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil.; };  
};
```

#### *Windows 2000/2003 DNS*

From the DNS management console snap-in, expand the Forward Lookup zones branch, select the zone you want to configure and right click and select Properties. Select the Zone Transfer tab.

If "Allow zone transfers:" is checked, "Only to the following servers" must also be checked. The reviewer must validate the name servers listed. If this is not the case, then this is a finding.

#### **Fix:** DNS0460

The DNS software administrator should configure each zone master server to limit zone transfers to a list of active slaves authoritative for that zone. Configuration details for BIND may be found in the DNS STIG Section 4.2.8.

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

---

<b>Vulnerability Key:</b>	V0004485
<b>STIG ID:</b>	DNS0470
<b>Vulnerability:</b>	A name server is not configured to only accept notifications of zone changes from a host authoritative for that zone.
<b>IA Controls:</b>	ECSC-1 Security Configuration Compliance
<b>Categories:</b>	4.6 DNS
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG

---

**Severity:** Category II

**Vulnerability Discussion:**

A slave updates its zone information by requesting a zone transfer from its master. In this transaction, the risk for the slave is that the response to its request is not in fact from its authorized master but from an adversary posing as the master. In this scenario, such an adversary would be able to modify and insert records into the slave's zone at will. To protect against this occurrence, the slave must be able to authenticate the master to provide assurance that any zone updates are valid.

**Check:** DNS0470

*BIND*

Instruction: If all of a zone's NS records are valid, then the default behavior in BIND complies with this requirement and does not require the DNS software administrator to take any additional action.

In some cases, the DNS software administrator must implement a non-default configuration to comply with operation requirements. If this is the case, the DNS software administrator must have an understanding of the named.conf options that govern how master name servers notify other hosts of zone changes and when slave servers will accept notifications. If none of these options are selected, the resulting behavior represents an acceptable security risk. If these phrases are configured, then this is a finding.

The phrases within the options statement that govern this behavior are:

- notify – which turns notification on or off (defaults to on)
- allow-notify – which defines from which servers a slave will accept notifications (defaults to the master name server only)

*Windows DNS*

Instruction: This check is not applicable to those Windows DNS Zones that are active directory integrated. Those zones will be replicated through active directory. For those servers running as a standard secondary zone, verify the name servers listed are only those authoritative for the zone. From the DNS management console snap-in, expand the Forward Lookup zones branch, select the zone you want to configure and right click and select Properties. Verify the entries under the Name Servers tab are only those authoritative for the zone.

In cases in which the name server is not running BIND or Windows DNS, the reviewer must still examine the configuration and its documentation to validate this requirement.

**Fix:** DNS0470

The DNS software administrator should configure a name server to only accept notifications of zone changes from a host authoritative for that zone. Configuration details may be found in the DNS STIG.

**OPEN:** ☐      **NOT APPLICABLE:** ☐      **FIXED:** ☐      **NOT A FINDING:** ☐

Comments:

<b>Vulnerability Key:</b>	V0004486
<b>STIG ID:</b>	DNS0475
<b>Vulnerability:</b>	Recursion is not prohibited on an authoritative name server.
<b>IA Controls:</b>	ECSC-1 Security Configuration Compliance
<b>Categories:</b>	4.6 DNS
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category II

**Vulnerability Discussion:**

A potential vulnerability of DNS is that an attacker can poison a name server's cache by sending queries that will cause the server to obtain host-to-IP address mappings from bogus name servers that respond with incorrect information. Once a name server has been poisoned, legitimate clients may be directed to non-existent hosts (which constitutes a denial of service) or, worse, hosts that masquerade as legitimate ones to obtain sensitive data or passwords. To guard against poisoning, name servers authoritative for .mil domains should be separated functionally from name servers that resolve queries on behalf of internal clients. Organizations may achieve this separation by dedicating machines to each function or, if possible, by running two instances of the name server software on the same machine; one for the authoritative function and the other for the resolving function. In this design, each name server process may be bound to a different IP address or network interface to implement the required segregation.

**Check:** DNS0475

*BIND*

Instruction: This check only applies if the name server is a master name server.

The reviewer should identify the recursion and allow-query phrases. They should look as follows:

```
Options {  
    recursion no;  
    allow-query {none;};  
};
```

```
Zone "example.com" {  
    Type master;  
    File "db.example.com";
```



```
Allow-query {none;};  
};
```

If either of these phrases is missing or have a value other than what is listed above, then this is a finding.

#### *Windows 2000/2003 DNS*

**Instruction:** This check only applies if the name server is a master name server, the Windows DNS servers are to only be configured as master name servers.

Open the DNS management console snap-in. Right click on the server and select properties. If available, under the forwarders tab (Windows 2000), ensure enable forwarders is not selected. If “Enable forwarders” is checked, this constitutes a finding.

Also examine the “Advanced” tab of the DNS server “Properties” dialog box. If “Disable recursion” is not checked, then this is a finding.

#### **Fix:** DNS0475

The DNS Administrator will configure the authoritative name server to prohibit recursion. Configuration details may be found in the DNS STIG. Client stub resolvers should be configured to query a recursive server for those outside of its local domain.

<b>OPEN:</b>	<input type="checkbox"/>	<b>NOT APPLICABLE:</b>	<input type="checkbox"/>	<b>FIXED:</b>	<input type="checkbox"/>	<b>NOT A FINDING:</b>	<input type="checkbox"/>
--------------	--------------------------	----------------------------	--------------------------	---------------	--------------------------	---------------------------	--------------------------

Comments:

<b>Vulnerability Key:</b>	V0004487
<b>STIG ID:</b>	DNS0480
<b>Vulnerability:</b>	A caching name server does not restrict recursive queries to only the IP addresses and IP address ranges of known supported clients.
<b>IA Controls:</b>	ECSC-1 Security Configuration Compliance
<b>Categories:</b>	4.6 DNS
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category II

**Vulnerability Discussion:**

Any host that can query a resolving name server has the potential to poison the servers name cache or take advantage of other vulnerabilities that may be accessed through the query service. The best way to prevent this type of attack is to limit queries to internal hosts, which need to have this service available to them.

**Check:** DNS0480

*BIND*

Instruction: This check is only applicable to caching name servers. Verify the allow-query and allow-recursion phrases are properly configured.

The reviewer should identify the allow-query and allow-recursion phrases. It should look as follows:

```
allow-query {trustworthy_hosts};  
allow-recursion {trustworthy_hosts};
```

The name of the ACL does not need to be “trustworthy\_hosts” but the name should match the ACL name defined earlier in named.conf for this purpose. If not, then this is a finding. The reviewer will also check for whether non-internal IP addresses appear in either the referenced ACL (e.g., trustworthy\_hosts) or directly in the statements themselves. If non-internal IP addresses do appear, then this is a finding.

*Windows 2000/2003 DNS*

Instruction: Windows 2000/2003 DNS should not be deployed as a caching name server. Consequently, the use of forwarders and recursion is prohibited on Windows DNS. The

reviewer will validate that the "Disable recursion" and the "Secure cache against pollution" on the "Advanced" tab of the name server properties are selected. Examine the "Advanced" tab of the DNS Server "Properties" dialog box. If "Disable recursion" and "Secure cache against pollution" is not checked, then this is a finding.

The reviewer will also validate, if available, that the "Enable forwarders" on the "Forwarders" tab of the name server properties is not selected. Examine the "Forwarders" tab of the DNS Server "Properties" dialog box. If "Enable forwarders" is checked, then this is a finding.

In cases in which the name server is not running BIND or Windows 2000/2003 DNS, the reviewer must still examine the configuration and its documentation to validate this requirement.

**Fix:** DNS0480

The DNS software administrator should configure the caching name server to accept recursive queries only from the IP addresses and address ranges of known supported. Client stub resolvers should be configured to query a recursive server for those outside of its local domain.

Configuration details for BIND and Windows DNS may be found in the DNS STIG.

<b>OPEN:</b>	<input type="checkbox"/>	<b>NOT APPLICABLE:</b>	<input type="checkbox"/>	<b>FIXED:</b>	<input type="checkbox"/>	<b>NOT A FINDING:</b>	<input type="checkbox"/>
--------------	--------------------------	----------------------------	--------------------------	---------------	--------------------------	---------------------------	--------------------------

Comments:

<b>Vulnerability Key:</b>	V0012774
<b>STIG ID:</b>	DNS0482
<b>Vulnerability:</b>	The forwarding configuration of DNS servers allows the forwarding of queries to servers controlled by organizations outside of the U.S. Government.
<b>IA Controls:</b>	ECSC-1 Security Configuration Compliance
<b>Categories:</b>	4.6 DNS
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category II

**Vulnerability Discussion:**

A side-effect of forwarding is that if the link between the forwarding server and the server to which queries are being forwarded is broken, DNS resolution will not work for the domain or domains being forwarded to the remote server. Query forwarding also allows the administrators of the remote server to change the DNS responses that are received by the clients of the forwarding servers. Organizations need to carefully configure any forwarding that is being used by their caching name servers. They should only configure "forwarding of all queries" to servers within the DoD. Systems configured to use domain-based forwarding should not forward queries for mission critical domains to any servers that are not under the control of the US Government.

**Check:** DNS0482

*BIND*

This check applies to caching servers only. Review the "options" statement in the named.conf file. The forwarders statement will have either a list of IP addresses or a name, which is defined by the ACL. Review the list of addresses for compliance. If they are outside of U.S. Government controlled IP address ranges, this is a finding. Some DNS servers are preconfigured, the defaults must be changed.

*Windows DNS:*

Windows DNS should not be deployed as a caching name server. Consequently, the use of forwarders is prohibited on Windows 2000/2003 DNS. Windows servers should not have any forwarding enabled. This can be configured from the client side stub resolver.

**Fix:** DNS0482

The SA will ensure the forwarding configuration of DNS servers does not forward queries to any servers controlled by organizations outside the US Government.

**OPEN:** ☐      **NOT  
APPLICABLE:** ☐      **FIXED:** ☐      **NOT A  
FINDING:** ☐

Comments:

---

**Vulnerability Key:** V0004488

**STIG ID:** DNS0485

**Vulnerability:** The DNS software does not log, at a minimum, success and failure of starting and stopping of the name server service daemon, zone transfers, zone update notifications, and dynamic updates.

**IA Controls:** ECAT-1 Audit trail, Monitoring, Analysis and Reporting  
ECAT-2 Audit trail, Monitoring, Analysis and Reporting

**Categories:** 10.2 Content Configuration

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category I/II

**Vulnerability Discussion:**

Logging must be comprehensive to be useful for both intrusion monitoring and security investigations. Setting logging at the severity notice should capture most relevant events without requiring unacceptable levels of data storage. The severity levels notice and debug are also available to organizations that require additional logging for certain events or applications.

**Check:** DNS0485

DNS software administrators need DNS transaction logs for a wide variety of reasons including troubleshooting, intrusion detection, and forensics. The events the name server logs are to contain, at a minimum, success and failure of the following events:

- start and stop of the name server service or daemon
- zone transfers
- zone update notifications
- dynamic updates

**BIND**

Instruction: For a BIND configuration: if a logging statement is present, it will have the form:

```
logging {  
    channel channel_name  
        file path_name | syslog syslog_facility  
severity (critical | error | warning |  
        notice | info | debug [level] | dynamic);
```

```
print-severity yes/no;  
print-time yes/no;  
};  
  
category category_name {  
    channel_name ; [ channel_name ; ...  
};  
};
```

Instruction: If a logging statement is not present, then this is a finding. The reviewer will look at the severity clause in each of the channel phrases of the logging statement. It should read either notice, info or debug for each defined channel (although debug would not typically appear unless the review is concurrent with a troubleshooting effort). If the logging statement is not properly configured, then this is a finding.

#### *Windows DNS*

Instruction: For a Windows 2000/2003 DNS configuration: On the “Logging Tab” or “Debug Logging” tab of the “DNS Server Properties” dialog box, if “Log Packets for debugging”, “Notifications”, and “Updates” are not checked, then this is a finding.

#### **Mitigation:** DNS0485

A violation of this requirement can have one of two severity levels depending upon the extent of the violation. If no logging exists, then the discrepancy would be a Category I finding. If some logging exists, but not for all of the events listed, then the discrepancy would be a Category II finding.

#### **Fix:** DNS0485

The DNS software administrator will configure the DNS software to log, at a minimum, success and failure of the following events:

- start and stop of the name server service or daemon
- zone transfers
- zone update notifications
- dynamic updates

Additional configuration details for BIND may be found in the DNS STIG Section 4.2.5 and configuration details for Windows 2000/ 2003 DNS may be found in the DNS STIG Section 5.7.

OPEN:	<input type="checkbox"/>	NOT APPLICABLE:	<input type="checkbox"/>	FIXED:	<input type="checkbox"/>	NOT A FINDING:	<input type="checkbox"/>
-------	--------------------------	--------------------	--------------------------	--------	--------------------------	-------------------	--------------------------

Comments:

---

**Vulnerability Key:** V0004489

**STIG ID:** DNS0490

**Vulnerability:** The DNS software administrator has not configured the DNS software to send all log data to either the system logging facility (e.g., UNIX syslog or Windows Application Event Log) or an alternative logging facility with security configuration equivalent to or more restrictive than the system logging facility.

**IA Controls:** COBR-1 Protection of Backup and Restoration Assets

**Categories:** 10.2 Content Configuration

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category II

**Vulnerability Discussion:**

On name servers, DNS log data is typically more sensitive than system log data and, consequently, should benefit from security controls at least as restrictive as those for the system logging facility. DNS software administrators require DNS transaction logs for a wide variety of reasons including troubleshooting, intrusion detection, and forensics. These logs should be appropriately secured, having file permissions that restrict unauthorized changes or viewing, and archived, being appropriately backed-up and stored in order for them to be examined at a future time. Furthermore, it is required that the logs be reviewed daily.

**Check:** DNS0490

DNS software administrators need DNS transaction logs for a wide variety of reasons including troubleshooting, intrusion detection, and forensics. These logs should be appropriately secured, having file permissions that restrict unauthorized changes or viewing, and archived, being appropriately backed-up and stored so that they can be examined at a future time.

**BIND**

The DNS software administrator will configure the DNS software to send all log data to either the system logging facility (e.g., UNIX syslog or Windows Application Event Log) or an alternative logging facility with security configuration equivalent to or more restrictive than the system logging facility.

Instruction: On an examination of the DNS configuration file (if BIND, named.conf), the reviewer can determine whether log data is sent to a facility other than the system logging facility. If this is the case, then the reviewer should do the following at a minimum:



- Compare the file permissions of the operating system logs with the file permissions of the alternative logging facility for DNS (e.g., using `ls -l`). If the permissions on the alternative are weaker in any manner, this constitutes a finding.
- Determine whether the system logs are transferred or copied to media on another machine (e.g., a cron job that periodically moves logs to another computer). If this is the case and there is not a similar technology in place for the DNS logs, then this constitutes a finding.

The reviewer can identify other ways in which the security of the DNS logs may be weaker than the security of the system logs, and can generate a finding based on that discovery so long as the explanation of the weakness is clearly documented in the SRR results.

#### *Windows DNS*

Windows DNS software log files will be equivalent to the system logging facility by default. In addition the dns debug log file should be checked at `%systemroot%\system32\dns\dns.log`. The permissions should be restricted to the Administrators group on the local computer or the Domain Admins group.

In cases in which the name server is not running BIND or Windows DNS, the reviewer must still examine the configuration and its documentation to validate this requirement.

#### **Fix:** DNS0490

The DNS software administrator should either configure `named.conf` to utilize the system logging facility or place additional technical controls (e.g., more restrictive file permissions) on the alternative logging facility so that it is as least as secure as the system logging facility.

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

---

**Vulnerability Key:** V0004490

**STIG ID:** DNS0495

**Vulnerability:** Entries in the name server logs do not contain timestamps and severity information.

**IA Controls:** ECAR-1 Audit Record Content  
ECAR-2 Audit Record Content  
ECAR-3 Audit Record Content

**Categories:** 10.2 Content Configuration

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:**

Forensic analysis of security incidents and day-to-day monitoring are substantially more difficult if there are no timestamps on log entries.

**Check:** DNS0495

*BIND*

Instruction: Based on the logging statement in named.conf, the reviewer can determine where the DNS logs are located. If their logging is not configured, then this is a finding. These logs (which in many cases are likely to be the system logs), should be viewed using the UNIX cat or tail commands, a text editor, or – in the case of Windows – the “Event Viewer.” When examining the logs, the reviewer should ensure that entries have timestamps and severity codes. If timestamps and severity codes are not found on one or more entries, then this is a finding.

```
logging {  
    channel channel_name  
        file path_name | syslog syslog_facility  
severity (critical | error | warning |  
    notice | info | debug [level] | dynamic);  
        print-severity yes/no;  
        print-time yes/no;  
    };  
    category category_name {  
        channel_name ; [ channel_name ; ...  
    };  
};
```

**Instruction:** If the DNS entries in the logs do not note their severity (i.e., critical, error, warning, notice, or info), then this constitutes a finding.

### *Windows DNS*

Windows DNS software adds timestamps and severity information by default.

In cases in which the name server is not running BIND or Windows DNS, the reviewer must still examine the configuration and its documentation to validate this requirement.

**Fix:** DNS0495

The DNS software administrator should configure the DNS software to add timestamps and severity information to each entry in all logs. Configuration details for BIND may be found in the DNS STIG Section 4.2.5.

<b>OPEN:</b>	<input type="checkbox"/>	<b>NOT APPLICABLE:</b>	<input type="checkbox"/>	<b>FIXED:</b>	<input type="checkbox"/>	<b>NOT A FINDING:</b>	<input type="checkbox"/>
--------------	--------------------------	----------------------------	--------------------------	---------------	--------------------------	---------------------------	--------------------------

Comments:

---

<b>Vulnerability Key:</b>	V0004491
<b>STIG ID:</b>	DNS0500
<b>Vulnerability:</b>	Valid root name servers do not appear in the local root zone file. G and H root servers, at a minimum, do not appear in the local root zone files.
<b>IA Controls:</b>	ECSC-1 Security Configuration Compliance
<b>Categories:</b>	4.6 DNS
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category I

**Vulnerability Discussion:**

All caching name servers must be authoritative for the root zone because without this starting point, they would have no knowledge of the DNS infrastructure and thus would be unable to respond to any queries. The security risk is that an adversary could change the root hints and direct the caching name server to a bogus root server. At that point, every query response from that name server is suspect, which would give the adversary substantial control over the network communication of the name servers clients. When authoritative servers are sent queries for zones that they are not authoritative for, and they are configured as a non-caching server (as recommended), they can either be configured to return a referral to the root servers or they can be configured to refuse to answer the query. The recommendation is to configure authoritative servers to refuse to answer queries for any zones for which they are not authoritative. This is more efficient for the server, and allows it to spend more of its resources doing what its intended purpose is; answering authoritatively for its zone. The security risk is that an adversary could change the root hints and direct the caching name server to a bogus root server. At that point, every query response from that name server is suspect, which would give the adversary substantial control over the network communication of the name server's clients.

**Check:** DNS0500

*BIND*

Instruction: This check is only applicable to caching name servers. Review the entries within the root hints file and validate that the entries are correct. Common names for the root hints file are root.hints, named.cache, or db.cache. The name is configurable within the named.conf file. Refer to the DNS Checklist for the correct entries.

*Windows DNS*

**Instruction:** This check only applies if the name server is a caching name server, the Windows DNS servers should only be configured as authoritative name servers. This requirement is only valid if the Windows DNS server is configured as a caching server, which would result in another finding. If the server is configured as a caching server, examine the DNS server properties by right clicking the server and selecting properties from the DNS Management console snap-in. Examine the entries under the Root Hints tab to ensure they are the same as the table below. These addresses are only valid for the NIPRNET.

In cases in which the name server is not running BIND or Windows DNS, the reviewer must still examine the configuration and its documentation to validate this requirement.

**Fix:** DNS0500

The DNS database administrator should configure the root hints file with these valid listed IP addresses.

Root Server	IP Address
A	198.41.0.4
B	192.228.79.201
C	192.33.4.12
D	128.8.10.90
E	192.203.230.10
F	192.5.5.241
G	192.112.36.4
H	128.63.2.53
I	192.36.148.17
J	192.58.128.30
K	193.0.14.129
L	199.7.83.42
M	202.12.27.33

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

---

**Vulnerability Key:** V0004492

**STIG ID:** DNS0505

**Vulnerability:** The DNS software administrator has not removed the root hints file on an authoritative name server in order for it to resolve only those records for which it is authoritative, and ensure that all other queries are refused.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 4.6 DNS

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:**

A potential vulnerability of DNS is that an attacker can poison a name server's cache by sending queries that will cause the server to obtain host-to-IP address mappings from bogus name servers that respond with incorrect information. The DNS architecture needs to maintain one name server whose zone records are correct and the cache is not poisoned. In this effort to prevent the authoritative name server from forwarding queries, is to delete the root hints. When authoritative servers are sent queries for zones that they are not authoritative for, and they are configured as a non-caching server (as recommended), they can either be configured to return a referral to the root servers or they can be configured to refuse to answer the query. The requirement is to configure authoritative servers to refuse to answer queries for any zones for which they are not authoritative. This is more efficient for the server, and allows it to spend more of its resources doing what its intended purpose is; answering authoritatively for its zone.

**Check:** DNS0505

*BIND*

Instruction: This check only applies if the name server is an authoritative name server. Ensure there is not a root hints on the name server. Common names for the root hints file are root.hints, named.cache, or db.cache. The name is configurable within the named.conf file.

*Windows DNS*

This check only applies if the name server is an authoritative name server. For a Windows 2000/2003 DNS configuration: Select the "Root Hints" Tab of the "DNS Server Properties" dialog box, ensure the root name server entries have been removed. The SA should, right click the entry and click the "Remove" button.

**Fix:** DNS0505

The SA should remove the root hints file. For a BIND installation, the SA should remove the root hints file. Common names for the root hints file are root.hints, named.cache, or db.cache. The name is configurable within the named.conf file.

For a Windows 2000/2003 DNS configuration, the SA should: Select the Root Hints Tab of the DNS Server Properties dialog box, to remove entries, right click the entry and click the Remove button.

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

---

**Vulnerability Key:** V0014756

**STIG ID:** DNS4600

**Vulnerability:** The DNS administrator will ensure non-routeable IPv6 link-local scope addresses are not configured in any zone. Such addresses begin with the prefixes of “FE8”, “FE9”, “FEA”, or “FEB”.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 4.6 DNS

**Responsibility:** DNS Administrator

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:**

IPv6 link local scope addresses are not globally routable and must not be configured in any DNS zone. Similar to RFC1918 addresses, if a link-local scope address is inserted into a zone provided to clients, most routers will not forward this traffic beyond the local subnet.

**Check:** DNS4600

#### *BIND*

- Instruction: Examine all zone statements contained in the *named.conf* file for a line containing the word *file* designating the actual file that stores the zones records. Examine the file that contains zones records for any IPv6 addresses containing the prefixes “FE8”, “FE9”, “FEA”, or “FEB”. If any link-local scope addresses are found, then this is a finding.

#### *Windows DNS*

- Instruction: From the windows task bar, select *Start, Programs/All Programs, Administrative Tools, DNS* to open the DNS management console. Expand the Forward Lookup Zones folder. Expand each zone folder and examine the host record entries. The third column titled Data will display the IP. Verify this column does not contain any IP address that begin with the prefixes “FE8”, “FE9”, “FEA”, or “FEB”.

**Fix:** DNS4600

The SA should remove any link-local addresses and replace with appropriate Site-Local or Global scope addresses.

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

---

**Vulnerability Key:** V0014757

**STIG ID:** DNS4610

**Vulnerability:** AAAA addresses are configured on a host that is not IPv6 aware.



**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 4.6 DNS

**Responsibility:** DNS Administrator

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:**

DNS is only responsible for resolving a domain name to an ip address. Applications and operating systems are responsible for processing the IPv6 or IPv4 record that may be returned. With this in mind, a denial of service could easily be implemented for an application that is not IPv6 aware. When the application receives an i.p. address in hexadecimal, it is up to the application/operating system to decide how to handle the response. Combining both IPv6 and IPv4 records into the same domain can lead to application problems that are beyond the scope of the DNS administrator.

**Check:** DNS4610

*BIND*

- Instruction: Examine all zone statements contained in the *named.conf* file for a line containing the word *file* designating the actual file that stores the zones records. Examine the file that contains zones records and verify IPv6 and IPv4 resource records are not in the same file. If the records are found in the same file, then this is a finding.

*Windows DNS*

Instruction: From the windows task bar, select *Start, Programs/All Programs, Administrative Tools, DNS* to open the DNS management console. Expand the Forward Lookup Zones folder. Expand each zone folder and examine the host record entries. The third column titled Data will display the IP. Verify this column does not contain both IPv4 and IPv6 addresses.

**Fix:** DNS4610

The SA should remove the IPv6 records from the IPv4 zone and create a second zone with only IPv6 records.

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:





## BIND RUNNING ON UNIX OR WINDOWS OS



**Vulnerability Key:** V0012440

**STIG ID:** DNS0250

**Vulnerability:** A new TSIG key is not generated and utilized for each type of transaction. (STIG has “new” and VMS has “unique”)

**IA Controls:** DCNR-1 Non-repudiation – Cryptography Standard

**Categories:** 4.6 DNS

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:** To enable zone transfer (requests and responses) through authenticated messages, it is necessary to generate a key for every pair of name servers. The key also can be used for securing other transactions, such as dynamic updates, DNS queries, and responses.

**Check:** DNS0250

Verify in the named.conf file that the key statement has a unique file name and location depending on transaction type.

**Fix:** DNS0250

The SA will ensure a new TSIG key is generated and utilized for each type of transaction (zone transfer, dynamic updates, etc)

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:

**Vulnerability Key:** V0004480

**STIG ID:** DNS0445

**Vulnerability:** A cryptographic key used to secure DNS transactions has been utilized on a name server for more than one year.

**IA Controls:** DCNR-1 Non-repudiation – Cryptography Standard

**Categories:** 8.4 Key Management

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category II

**Vulnerability Discussion:**

Keys are more likely to be compromised if they remain in use for over a year.

**Check:** DNS0445

Instruction: With the SA's assistance, the reviewer should locate the file directory that contains the TSIG keys (i.e., /etc/dns/keys/) and then list the files in that directory (e.g., by using the UNIX ls -l command). The key statements in named.conf will provide the location of the key files. If any of them have a last modified time stamp that is more than one year old, then this is a finding.

**Fix:** DNS0445

The IAO should execute the organizations procedure for TSIG key supersession.

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:

<b>Vulnerability Key:</b>	V0004493
<b>STIG ID:</b>	DNS0705
<b>Vulnerability:</b>	The DNS software administrator has not utilized at least 160-bit HMAC-SHA1 keys .
<b>IA Controls:</b>	DCNR-1 Non-repudiation
<b>Categories:</b>	8.4 Key Management
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category III

**Vulnerability Discussion:**

Current versions of BIND do include support for SHA-1, which is the algorithm currently specified in the National Institute of Standards and Technology's (NISTs) Secure Hashing Standard (FIPS 180-1) and required throughout DoD. Hmac md5 will be replaced with hmac-sha1 or higher for DNS TSIG applications. In general, only NIST or National Security Agency (NSA) approved algorithms should be utilized in the DoD computing infrastructure. The US Government currently requires SHA-1 for hashing applications. It is considered an improvement over MD5, for which there are known instances of collisions.

**Check:** DNS0705

There is to be a properly configured key statement located in the named.conf file.

BIND now supports HMAC-SHA1 and organizations are required to migrate to this algorithm or greater.

An example of a properly configured key statement in practice might be:

```
key ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil {  
    algorithm hmac-sha1;  
    include "/etc/dns/keys/ns1_ns2.key";  
};
```

If the key statement is not configured, then this is a finding.

If the key statement is not configured to implement least HMAC-SHA1, then this is a finding.

**Fix:** DNS0705

The DNS software administrator should include the phrase algorithm HMAC-SHA1 or greater in each key statement depending upon which is currently available.

**OPEN:** ☐      **NOT APPLICABLE:** ☐      **FIXED:** ☐      **NOT A FINDING:** ☐

Comments:

<b>Vulnerability Key:</b>	V0004494
<b>STIG ID:</b>	DNS0710
<b>Vulnerability:</b>	A TSIG key is not in its own dedicated file.
<b>IA Controls:</b>	ECCD-1 Changes to Data ECCD-2 Changes to Data
<b>Categories:</b>	2.1 Object Permissions
<b>Severity:</b>	Category II

**Vulnerability Discussion:**

Ideally, nobody even DNS and Systems Administrators should view the key. If it is included in named.conf, they will view it on a regular basis, which means computer forensics is less likely to determine who may have obtained the key if it is compromised. In addition, if the named.conf needs to be copied from the system for whatever reason (e.g., sent to an expert to troubleshoot a problem, appended to a change management work order, etc.), then others will see the key and could copy it. On the other hand, if the key is in a dedicated file, then the operating system can be configured to log any instance when the key is accessed, which would make it easy for security personnel to determine when users other than the DNS name server software performed this function.

**Responsibility:** System Administrator

**References:** DNS STIG

**Check:** DNS0710

The key statement is located in the named.conf. If the key statement includes a secret phrase followed by a character representation of the key, then this is a finding. The correct configuration calls for an include statement embedded in the key statement. The include statement references a separate file that contains the key so it does not need to appear in the named.conf file.

An example of a properly configured key statement in practice might be:

```
key ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil {  
    algorithm hmac-md5;  
    include "/etc/dns/keys/ns1_ns2.key";  
};
```

If each key is not located in a dedicated file for each individual key, then this is a finding.

**Fix:** DNS0710



The DNS software administrator should cut and paste the secret phrase from each key statement and place it in a dedicated file. Then, an include phrase should be added to the key statement.

Additional information on TSIG key generation and storage may be obtained from the DNS STIG.

Create a new designated file for that key

Using a text editor, create a file with the following content:

```
secret "generated_key";
```

In our example, the contents would be:

```
secret "2njlQNnzn6HTwKLcjStUXg==";
```

The syntax of the statement is critical. Ensure that:

- The word "secret" appears at the beginning of the line followed by a space
- The key is included in quotes with no extra spaces before or after the key
- A semi-colon (;) follows the quotation mark after the key
- There are no extra characters, lines, or carriage returns before or after the statement

Importantly, any key longer than approximately 320 bits will contain a space within the key field of the original .key file. This space can be left within the string, as long as it is enclosed within double quotes (") in the new file created to house the key.

<b>OPEN:</b>	<input type="checkbox"/>	<b>NOT APPLICABLE:</b>	<input type="checkbox"/>	<b>FIXED:</b>	<input type="checkbox"/>	<b>NOT A FINDING:</b>	<input type="checkbox"/>
--------------	--------------------------	----------------------------	--------------------------	---------------	--------------------------	---------------------------	--------------------------

Comments:

**Vulnerability Key:** V0004511

**STIG ID:** DNS0715

**Vulnerability:** A BIND name server is not configured to accept control messages only when the control messages are cryptographically authenticated and sent from an explicitly defined list of DNS administrator workstations.

**IA Controls:** DCNR-1 Non-repudiation – Cryptography Standard

**Categories:** 2.2 Least Privilege

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category II

**Vulnerability Discussion:**

The controls statement and the associated use of the `rndc` or `ndc` commands introduces the risk that an adversary could use them to remotely control the name server without having to authenticate to the operating system on which the name server resides.

**Check:** DNS0715

If control messages are utilized, there is to be a properly configured keys statement within the controls statement located in the `named.conf`.

An example of a properly configured controls statement in practice might be:

```
controls {  
    inet 127.0.0.1  
    allow 127.0.0.1  
    keys { "rndc_key" };  
};
```

If control messages are utilized and not cryptographically authenticated, then this is a finding.

**Fix:** DNS0715

If control messages are utilized, the DNS software administrator should properly configure the allow and keys phrases within the controls statement located in the `named.conf` to properly authenticate the control messages.

`rndc` also has its own configuration file, `rndc.conf`, that has a similar syntax to the `named.conf` file, but is limited to the options, key, server, and include statements. An example of a minimal configuration is as follows:

```
key rndc_key {  
    algorithm hmac-md5;  
    secret "2njlQNzn6HTwKLcjStUXg==";  
};  
options {  
    default-server localhost;  
    default-key rndc_key;
```

**OPEN:** ☐      **NOT APPLICABLE:** ☐      **FIXED:** ☐      **NOT A FINDING:** ☐

Comments:

---

<b>Vulnerability Key:</b>	V0004495
<b>STIG ID:</b>	DNS0720
<b>Vulnerability:</b>	A unique TSIG key is not utilized for communication between name servers sharing zone information.
<b>IA Controls:</b>	DCNR-1 Non-repudiation – Cryptography Standard
<b>Categories:</b>	8.4 Key Management
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category II

**Vulnerability Discussion:**

If a secret key shared between two servers is not unique, then any breach of the key is not limited to those two servers. In particular, if all servers in a zone share the same key, then there is the possibility that an attack could modify records in all of the servers. Recovering from a successful attack is considerably more difficult in this circumstance. Furthermore, the more copies of any one key are in existence, the greater the likelihood that the confidentiality of that key will be lost at some point in time.

**Check:** DNS0720

Two name servers sharing zone information must utilize a unique TSIG key for communication between them or, in cases in which more than four servers support a zone, create a written key management plan that will document how keys are shared and replaced in a manner to reduce residual risk to an acceptable level.

If there are no server statements within named.conf, this is a finding. If there are server statements, then check that there is one corresponding to each of the zone partners. If this is not the case, then this is also a finding.

If there are server statements for servers other than those supplied, then there may be a finding associated with the incompleteness of the list.

On the master name server, this is an example of a configured key statement:

```
key ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil. {  
  algorithm hmac-md5;  
  include "/etc/dns/keys/tsig-example.key";  
};
```

```
zone "disa.mil" {  
    type master;  
    file "db.disa.mil";  
allow-transfer { key ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil.; };  
};
```

On the slave name server, this is an example of a configured key statement:

```
key ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil. {  
    algorithm hmac-md5;  
    include "/etc/dns/keys/tsig-example.key";  
};  
  
server 10.2.2.2 {  
    keys { ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil };  
};  
  
zone "disa.mil" {  
    type slave;  
    masters { 10.1.1.1; };  
    file "db.disa.mil";  
};
```

Check the keys phrase within each of the server statements to ensure uniqueness of keys. If two or more server statements reference the same key, then this is a finding.

**Fix:** DNS0720

The DNS software administrator should modify the named.conf and server statements so that the key shared between any two servers is unique. This may involve the generation of additional keys and the creation of new files dedicated to those keys.

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

---

**Vulnerability Key:** V0014758

**STIG ID:** DNS4620

<b>Vulnerability:</b>	The DNS software administrator will ensure the <code>named.conf</code> options statement does not include the option "listen-on-v6 { any; };" when an IPv6 interface is not configured and enabled.
<b>IA Controls:</b>	ECSC-1 Security Configuration Compliance
<b>Categories:</b>	4.6 DNS
<b>Responsibility:</b>	DNS Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category II

#### **Vulnerability Discussion:**

To prevent the possibility of a denial of service in relation to an IPv4 DNS server trying to respond to IPv6 request, the server should be configured to not listen on any of its IPv6 interfaces unless it does contain IPv6 AAAA resource records in one of the zones.

**Check:** DNS4620

#### *BIND on UNIX*

- Instruction: Examine the *named.conf* file which usually resides in the */etc* directory. Perform the following command to check if IPv6 is enabled for BIND.

```
# grep -c "listen-on-v6" named.conf
```

This will return the number of entries found in the `named.conf` file. If the number is greater than zero, proceed to check if any IPv6 interfaces are configured. Execute the following to check for IPv6 interfaces.

```
# ifconfig -a
```

#### *BIND on Windows*

- Instruction: Ask the SA the location of the `named.conf`. This is configured on the initial installation of ISC BIND. Right click on the file and select *open with*. Select *notepad* or *wordpad* to open the file. Use Ctrl+F and enter "listen-on-v6" at the prompt. If any entries are found, then check for any enabled IPv6 interfaces on the machine. Perform the following to check:
  - Click **Start**, click **Control Panel**, and the double-click **Network Connections**.
  - Right-click any local area connection, and then click **Properties**.
  - The display will contain, **Microsoft TCP/IP version 6** with a check next to the item if IPv6 is installed..

**Fix:** DNS4620

The DNS administrator should remove the “listen-on-v6” option from the named.conf file if there are no interfaces configured in the operating system for IPv6..

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

---

**Vulnerability Key:** V0014759

**STIG ID:** DNS4640

**Vulnerability:** The DNS administrator, when implementing DNSSEC, will create and maintain separate key-pairs for key signing and zone signing.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 4.6 DNS

**Responsibility:** DNS Administrator

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:** DNSSEC specifies generation and verification of digital signatures using asymmetric keys. This requires generation of a public key-private key pair. Although the DNSSEC specification does not call for different keys (just one key pair), experience from pilot implementations suggests that for easier routine security administration operations such as key rollover (changing of keys) and zone re-signing, at least two different types of keys are needed.

**Check:** DNS4640

*BIND*

**Instruction:** : Examine the DNSKEY records in the zone file. At least two should exist display different keys in the eighth field.

```
example.com.      86400 IN      DNSKEY      256 3 1      aghaghnl;knatnjkga;agn;g'a
example.com.      86400 IN      DNSKEY      256 3 1      grupotqtuiptqiqtouqptuqv1l
```

**Fix:** DNS4640

Generate a new KSK pair and update the DNSKEY record with the following:

```
# dnssec-keygen -n ZONE -a RSA -b 2048 example.com
```

Generate a new ZSK pair and update the DNSKEY record with the following:

```
# dnssec-keygen -n ZONE -a RSA -b 1024 example.com
```

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:

---

**Vulnerability Key:** V0014760

**STIG ID:** DNS4650

**Vulnerability:** The DNSSEC algorithm for digital signatures is not RSASHA1.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 4.6 DNS

**Responsibility:** DNS Administrator

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:** Due to its wide availability and performance. RSASHA1 is the preferred algorithm for zone signatures.

**Check:** DNS4650



## *BIND*

Instruction: Examine the DNSKEY record in the zone file. The seventh field will contain a number representing the algorithm used to generate the key. If this number is not a five, then this is a finding. Here is an example:

```
example.com.      86400 IN      DNSKEY      256 3 5      aghaghnl;knatnjkga;agn;g'a
```

### **Fix:** DNS4650

Generate a new key pair and update the DNSKEY record with the following:

```
# dnssec-keygen -n ZONE -a RSASHA1 -b 2048 example.com
```

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

---

**Vulnerability Key:** V0014761

**STIG ID:** DNS4660

**Vulnerability:** The DNSSEC key signing key is not at least 2048 bits.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 4.6 DNS

**Responsibility:** DNS Administrator

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:** The choice of key size is a tradeoff between the risk of key compromise and performance. The performance variables are signature generation and verification times. The size of the DNS response packet also is a factor because DNSKEY RRs may be sent in the additional section of the DNS response. Because the KSK is used only for signing the key set (DNSKEY RRSet), performance is not much of an issue. Compromise of a

KSK could have a great impact, however, because the KSK is the entry point key for a zone. Rollover of a KSK in the event of a compromise involves potential update of trust anchors in many validating resolvers. Hence, a large key size is recommended for the KSK. A large key size decreases the chances of the key compromise and avoids the need for frequent rollovers as each rollover requires administrative monitoring and follow-up action.

**Check:** DNS4660

**BIND**

Instruction: Examine the public key record type DNSKEY in the zone file. The actual key contained in the file utilizing the RSA algorithm and a key size of 2048 bits will contain 351 characters. If the key does not appear to contain at 351 characters, then this is a finding.

**Fix:** DNS4660

Generate a new key pair and update the DNSKEY record with the following:  
# dnssec-keygen -n ZONE -a RSA -b 2048 example.com

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

---

**Vulnerability Key:** V0014762

**STIG ID:** DNS4670

**Vulnerability:** The DNSSEC key signing key does not have a minimum roll over period of one year.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 4.6 DNS

**Responsibility:** DNS Administrator

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:** A good practice is to generate an extra set of key signing keys for rollover purposes. The additional key will be readily available for emergency situations such as key compromise. The key signing key should be rolled over on an annual basis.

**Check:** DNS4670

*BIND on UNIX*

Instruction: Ask the DNS administrator for the location of the private key file for the KSK generated from the output of the dnssec-keygen command. Perform the following:

```
# ls -la 'private_key_file'
# date
```

If the date returned compared to the date on the file is greater than a year, then this is a finding.

*BIND on Windows*

Instruction: Ask the DNS administrator for the location of the private key file for the KSK generated from the output of the dnssec-keygen command.  
Perform the following:

Right click on the file and select **Properties**.  
Select the **General** tab and view *Created:* row which displays the date of creation.  
Check the date of the machine in the lower right hand corner of the display.  
Compare the dates; if the difference is greater than a year, then this is a finding.

**Fix:** DNS4670

Generate new keys with the following command:  
# dnssec-keygen -n ZONE -a RSASHA1 -b 2048 example.com

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

---

**Vulnerability Key:** V0014764

**STIG ID:** DNS4680

**Vulnerability:** The DNSSEC zone signing key size is not at least 1024 bits.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 4.6 DNS

**Responsibility:** DNS Administrator

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:** As far as the choice of key size for the ZSK is concerned, performance certainly will be a factor because the ZSK is used for signing all RRsets in the zone. In terms of impact, however, it is restricted to just a single zone because the ZSK.s usage is limited to signing RRsets only for that zone but not for providing authenticated delegation for a child zone. Hence, a key size smaller than that for the KSK can be used for the ZSK.

**Check:** DNS4680

#### *BIND*

Instruction: Examine the public key record type DNSKEY in the zone file. The actual key contained in the file utilizing the RSA algorithm and key size of 1024 bits will contain 180 characters. If the key does not appear to contain at 180 characters, then this is a finding.

**Fix:** DNS4680

Generate a new key pair and update the DNSKEY record with the following:  
# dnssec-keygen -n ZONE -a RSA -b 1024 example.com

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

---

**Vulnerability Key:** V0014765

**STIG ID:** DNS4690

<b>Vulnerability:</b>	The DNSSEC zone signing key minimum roll over period is not at least 60 days.
<b>IA Controls:</b>	ECSC-1 Security Configuration Compliance
<b>Categories:</b>	4.6 DNS
<b>Responsibility:</b>	DNS Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category III

**Vulnerability Discussion:** In the case of ZSK, the risk of key guessing is higher because of larger key exposure. The larger key exposure is a result of the fact that the number of signature sets generated is very large (because the ZSK signs all RRsets in a zone and other RRsets change much more frequently than DNSKEY RRsets, so the number of fresh signatures generated is high). This factor, combined with the relatively smaller size of the key, implies that ZSKs must be rolled over more frequently than KSKs (usually a month or two).

**Check:** DNS4690

#### *BIND on UNIX*

Instruction: Ask the DNS administrator for the location of the private key file for the ZSK generated from the output of the dnssec-keygen command. Perform the following:

```
# ls -la 'private_key_file'
# date
```

If the date returned compared to the date on the file is greater than 60 days, then this is a finding.

#### *BIND on Windows*

Instruction: Ask the DNS administrator for the location of the private key file for the ZSK generated from the output of the dnssec-keygen command.  
Perform the following:

Right click on the file and select **Properties**.  
Select the **General** tab and view *Created:* row which displays the date of creation.  
Check the date of the machine in the lower right hand corner of the display.  
Compare the dates, if the difference is greater than 60 days, then this is a finding.

**Fix:** DNS4690

Generate new keys with the following command:  
# dnssec-keygen -n ZONE -a RSA -b 1024 example.com

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:

---

**Vulnerability Key:** V0014766

**STIG ID:** DNS4700

**Vulnerability:** The DNSSEC private key file permissions are not owned by the DNS administrator or the permissions are not set to a minimum of 600.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 4.6 DNS

**Responsibility:** DNS Administrator

**References:** DNS STIG

**Severity:** Category I

**Vulnerability Discussion:** The private keys in the KSK and ZSK key pairs should be protected from unauthorized access. If possible, the private keys should be stored offline (with respect to the DNSSEC-aware name server) in a physically secure, non-network-accessible machine along with the zone file master copy. The signatures generated by using the private keys should be transferred to the primary authoritative name servers through a load process, using a dynamically established network connection (rather than a permanent network link).

**Check:** DNS4700

*BIND on UNIX*

- Instruction: Ask the DNS administrator for the directory location containing the private key files. Perform the following to check the permissions:  
# ls -la 'key file'

If the owner of the file is not the DNS administrator or the permissions are weaker than 600, then this is a finding.

### *BIND on Windows*

- **Instruction:** Ask the DNS administrator for the directory location containing the private key files. Right click on the file and select **Properties**. Under the file properties, select the **Security** tab. Ensure the Administrator group has **full control** and the DNS user has **read** permission.

**Fix:** DNS4700

For UNIX systems:

```
# chown dnsadmin 'keyfile'
```

```
# chmod 600 'keyfile'
```

For Windows systems:

Ask the DNS administrator for the directory location containing the private key files. Right click on the file and select **Properties**. Under the file properties, select the **Security** tab. Ensure the Administrator group has **full control** and the DNS user has **read** permission.

**OPEN:** ☐

**NOT  
APPLICABLE:** ☐

**FIXED:** ☐

**NOT A  
FINDING:** ☐

Comments:

<b>Vulnerability Key:</b>	V0014767
<b>STIG ID:</b>	DNS4710
<b>Vulnerability:</b>	DNSSEC is not enabled for signing files between name servers with DNSSEC capabilities.
<b>IA Controls:</b>	ECSC-1 Security Configuration Compliance
<b>Categories:</b>	4.6 DNS
<b>Responsibility:</b>	DNS Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category II

**Vulnerability Discussion:** A powerful feature of DNSSEC is the ability to sign record sets to ensure their integrity and authenticity throughout the DNS infrastructure and not just between the authoritative name server and its zone partner or local client. The advantages of this feature become apparent when DoD users wish to securely validate records from other organizations, including commercial vendors, business partners, and other Government agencies.

**Check:** DNS4710

*BIND*

- Instruction: Ask the DNS administrator for the directory location containing *named.conf* file  
Check for the following option:

```
options {  
    dnssec-enable yes; };
```

If the option is set to no or not in the *named.conf* file, then this is a finding.

**Fix:** DNS4710

Ensure BIND 9.3.1. is installed with DNSSEC support. Add the following entry to *named.conf*.

```
options {  
    dnssec-enable yes; };
```

OPEN:	<input type="checkbox"/>	NOT APPLICABLE:	<input type="checkbox"/>	FIXED:	<input type="checkbox"/>	NOT A FINDING:	<input type="checkbox"/>
-------	--------------------------	--------------------	--------------------------	--------	--------------------------	-------------------	--------------------------

Comments:





### 3.1 BIND on UNIX Only



**Vulnerability Key:** V0003617

**STIG ID:** DNS4440

**Vulnerability:** BIND is not configured to run as a dedicated non-privileged user account. BIND is running as a root user.

**IA Controls:** ECLP-1 Least Privilege

**Categories:** 2.2 Least Privilege

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:**

If an intruder gains control of named (BIND), the intruder will acquire the privileges of the user ID under which it runs. Running as a non-privileged user account limits the extent of any breach. When BIND runs as root (the default) intruders gain full control of the system.

**Check:** DNS4440

In the presence of the reviewer, the SA should enter the following command:

```
ps -ef | grep 'named' > /etc/dns/srr/bindUser.srr
```

The user identification (UID) utilized to run named should be found in the results. If the UID is root (i.e., 0) or another built-in ID, then this constitutes a finding. If it is not, then the next step is to check whether the UID is dedicated to this function. The SA should enter the following command, substituting the UID obtained in the previous step for bindUID:

```
ps -ef | grep 'bindUID' > bindUserDaemons.srr
```

If bindUserDaemons.tmp contains daemons/programs other than BIND (named), then this constitutes a finding. If the dedicated user is associated with named only, the next step is to check whether the user ID has any privileges other than those needed to run BIND. To accomplish this, the SA will check the following:

- Whether the BIND UID is a member of any group other than dnsgroup.

- Whether the BIND UID has permissions to any files other than key files and named.stat.

For the first item, the SA should run the following command (substituting the value for bindUID as appropriate):

```
grep 'bindUID' /etc/group > /etc/dns/srr/bindUserGroups.srr
```

For the second item, the SA should run the following command (substituting the name of the user ID for dnsuser if applicable):

```
find / -uid bindUID > /etc/dns/srr/bindUserFiles.srr
```

With regards to the first item, if dnsuserGroups.srr contains any entry other than dnsgroup (or its equivalent), then this constitutes a finding. With regards to the second item, if dnsuserFilePermissions.srr contains any entries other than the key files and named.stat, then this constitutes a finding.

**Fix:** DNS4440

The SA should create a new user account dedicated to DNS, configure it per the DNS STIG, and then restart the named process to run as a the new user account.

OPEN:	<input type="checkbox"/>	NOT APPLICABLE:	<input type="checkbox"/>	FIXED:	<input type="checkbox"/>	NOT A FINDING:	<input type="checkbox"/>
-------	--------------------------	--------------------	--------------------------	--------	--------------------------	-------------------	--------------------------

Comments:

<b>Vulnerability Key:</b>	V0012967
<b>STIG ID:</b>	DNS4445
<b>Vulnerability:</b>	The SA has not configured BIND in a chroot(ed) directory structure.
<b>IA Controls:</b>	ECLP-1 Least Privilege
<b>Categories:</b>	4.6 DNS
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category III

**Vulnerability Discussion:**

With any network service, there is the potential that an attacker can exploit a vulnerability within the program that allows the attacker to gain control of the process and even run system commands with that control. One possible defense against this attack is to limit the software to particular quarantined areas of the file system, memory or both. This effectively restricts the service so that it will not have access to the full file system. If such a defense were in place, then even if an attacker gained control of the process, the attacker would be unable to reach other commands or files on the system. This approach often is referred to as a padded cell, jail, or sandbox. All of these terms allude to the fact that the software is contained in an area where it cannot harm either itself or others. A more technical term is a chroot(ed) directory structure. BIND should be configured to run in a padded cell or chroot(ed) directory structure if supported by the operating system

**Check:** DNS4445

Review the startup file and make sure the -t option is included:

Edit the startup files to start named with the -t option and option argument: -t /var/named.  
Similarly to syslogd, many modern versions of UNIX start named from /etc/rc.d/init.d/named.

**Fix:** DNS4445

The SA will ensure BIND is configured in a chroot(ed) directory structure.

<b>OPEN:</b>	<input type="checkbox"/>	<b>NOT</b>	<input type="checkbox"/>	<b>FIXED:</b>	<input type="checkbox"/>	<b>NOT A</b>	<input type="checkbox"/>
		<b>APPLICABLE:</b>				<b>FINDING:</b>	

Comments:

<b>Vulnerability Key:</b>	V0003618
<b>STIG ID:</b>	DNS4450
<b>Vulnerability:</b>	A UNIX or UNIX-based name server is running unnecessary daemon/services and/or is configured to start an unnecessary daemon, service, or program upon boot up.
<b>IA Controls:</b>	ECSC-1 Security Configuration Compliance
<b>Categories:</b>	14.4 Unneeded Ports, Protocols, Hardware, and Services
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category II

**Vulnerability Discussion:**

Unnecessary software running on a name server could introduce security vulnerabilities that would be avoided if it were not present.

**Check:** DNS4450

The reviewer should examine the start-up files to determine whether they launch unnecessary programs. The file `/etc/inetd.conf` is common to UNIX implementations. The reviewer may use the `cat` command to view this file. If the file contains any of the daemons listed, this is a finding:

If SNMP is used for network management it must be documented and configured in accordance with the UNIX STIG.

Below is a list of prohibited services. If any of these processes are running (the reviewer may use the `ps -ef | grep service name` to verify if the process is running or not), or configured to be started upon boot-up (the reviewer may use the `ls` command in the `/etc/rc2.d` or `/etc/rc3.d` directory), then this is a finding (although inherently dangerous, if SNMP is used for network management purposes, it must be documented and configured in accordance with the UNIX STIG):

- NFS client (`s73nfs.client` in `rc2.d`)
- automounter (`s74autofs` in `rc2.d`)
- printer queue daemon (`s80lp` in `rc2.d`)
- RPC portmapper (`s71rpc` in `rc2.d`)
- CDE login (`s99dtlogin` in `rc2.d`)
- NFS server process (`s15nfs.server` in `rc3.d`)
- SNMP daemon (`s76snmpdx` in `rc3.d`)

**Mitigation:**

If SNMP is used for network management it must be documented and configured in accordance with the UNIX STIG. SNMP is not a finding if operationally necessary and documented as such.

**Fix:** DNS4450

The SA should edit startup files (e.g., inetd.conf) so that the unnecessary programs do not launch on boot-up.

<b>OPEN:</b>	<input type="checkbox"/>	<b>NOT APPLICABLE:</b>	<input type="checkbox"/>	<b>FIXED:</b>	<input type="checkbox"/>	<b>NOT A FINDING:</b>	<input type="checkbox"/>
--------------	--------------------------	----------------------------	--------------------------	---------------	--------------------------	---------------------------	--------------------------

Comments:

**Vulnerability Key:** V0003619

**STIG ID:** DNS4460

**Vulnerability:** It is possible to obtain a command shell by logging on to the DNS user account.

**IA Controls:** ECLP-1 Least Privilege

**Categories:** 2.2 Least Privilege

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:**

If an intruder gains access to a command shell, the intruder may be able to execute unauthorized commands.

**Check:** DNS4460

The SA should enter the following command (this command assumes that named is running as user dnsuser):

```
grep dnsuser /etc/passwd
```

Based on the command output, the reviewer can identify whether a shell exists for dnsuser. The shell should be /dev/null or /bin/false. If it is a legitimate shell, then this is a finding.

**Fix:** DNS4460

The SA should edit /etc/passwd and change the shell of the DNS user account to /bin/false, /dev/null, or an alternative producing a similar effect.

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:

---

**Vulnerability Key:** V0003620

**STIG ID:** DNS4470

**Vulnerability:** Permissions on critical UNIX name server files are not as restrictive as required.

**IA Controls:** ECCD-1 Changes to Data  
ECCD-2 Changes to Data

**Categories:** 2.1 Object Permissions

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category II

**Vulnerability Discussion:**

Weak permissions could allow an intruder to view or modify zone, configuration and/or program files.

**Check:** DNS4470

Using the `ls -l` command from the directory containing the core BIND files, check that the permissions for the files listed are at least as restrictive as those listed:

<i>FILE NAME</i>	<i>OWNER</i>	<i>GROUP</i>	<i>PERMISSIONS</i>
<i>named.conf</i>	<i>root</i>	<i>dnsgroup</i>	<i>640</i>
<i>named.pid</i>	<i>root</i>	<i>dnsgroup</i>	<i>600</i>
<i>Root hints file</i>	<i>root</i>	<i>dnsgroup</i>	<i>640</i>
<i>master zone file</i>	<i>root</i>	<i>dnsgroup</i>	<i>640</i>
<i>slave zone file</i>	<i>root</i>	<i>dnsgroup</i>	<i>660</i>

The name of the root hints file is defined in `named.conf`. Common names for the file are `root.hints`, `named.cache`, or `db.cache`.

**Fix:** DNS4470

The SA should modify permissions so that they are at least as restrictive as specified in the DNS STIG.

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

---



**Vulnerability Key:** V0012966

**STIG ID:** DNS4480

**Vulnerability:** Inadequate file permissions on BIND name servers.

**IA Controls:** ECCD-1 Changes to Data  
ECCD-2 Changes to Data

**Categories:** 2.1 Object Permissions

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category II

**Vulnerability Discussion:**

Weak permissions could allow an intruder to view or modify zone, configuration and/or program files.

**Check:** DNS4480

On BIND name servers, the following permissions must be set:

<i><b>FILE NAME</b></i>	<i><b>OWNER</b></i>	<i><b>GROUP</b></i>	<i><b>PERMISSIONS</b></i>
<i>named.run</i>	<i>root</i>	<i>dnsgroup</i>	<i>660</i>
<i>named_dump.db</i>	<i>root</i>	<i>dnsgroup</i>	<i>660</i>
<i>ndc (FIFO)</i>	<i>root</i>	<i>dnsgroup</i>	<i>600</i>
<i>ndc.d (directory containing ndc)</i>	<i>root</i>	<i>dnsgroup</i>	<i>700</i>

The following must be set on log files:

<i><b>FILE NAME</b></i>	<i><b>OWNER</b></i>	<i><b>GROUP</b></i>	<i><b>PERMISSIONS</b></i>
<i>any log file</i>	<i>dnsuser</i>	<i>dnsgroup</i>	<i>660</i>

The following must be set on TSIG keys:

<i><b>FILE NAME</b></i>	<i><b>OWNER</b></i>	<i><b>GROUP</b></i>	<i><b>PERMISSIONS</b></i>
<i>unique to each key</i>	<i>dnsuser</i>	<i>dnsgroup</i>	<i>400</i>

**Fix:** DNS4480

The SA will ensure that the file permissions on BIND files as well as the log and TSIG key files are set in accordance with the DNS STIG requirements.

**OPEN:** ☐ **NOT** ☐  
**APPLICABLE:** ☐ **FIXED:** ☐ **NOT A** ☐  
**FINDING:** ☐

Comments:

## 3.2 BIND on Windows Only



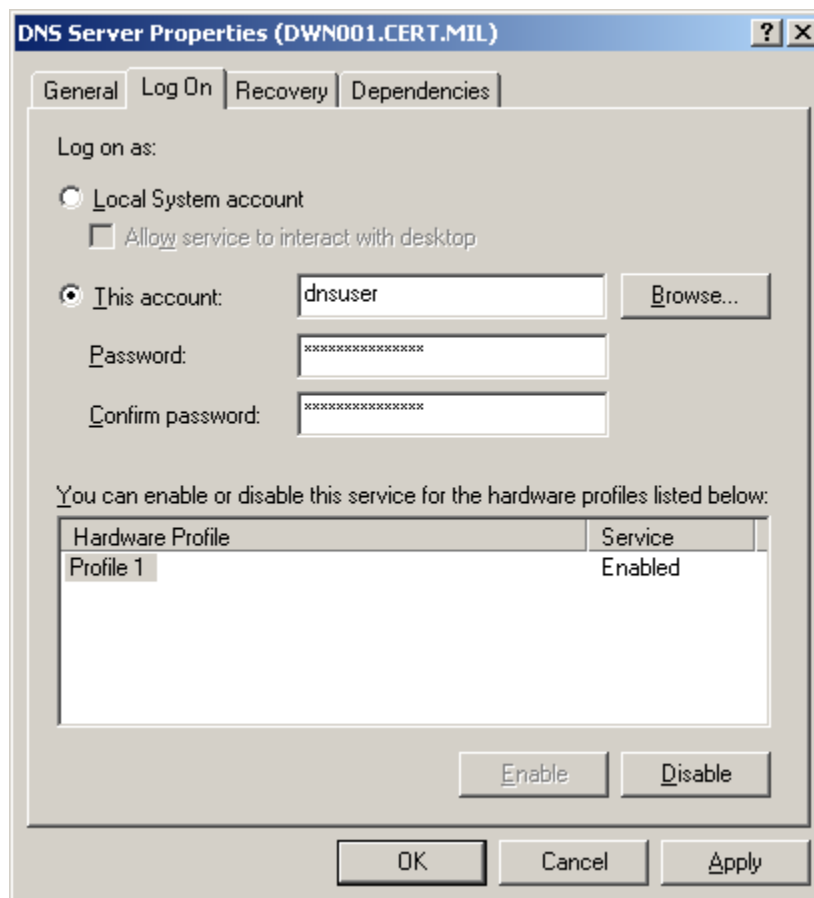
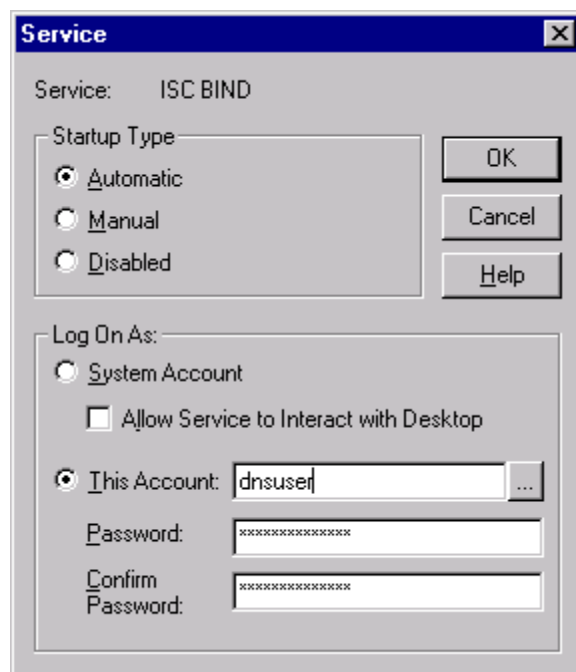
<b>Vulnerability Key:</b>	V0003621
<b>STIG ID:</b>	DNS4530
<b>Vulnerability:</b>	ISC BIND is not configured to run as a dedicated non-privileged service user account.
<b>IA Controls:</b>	ECLP-1 Least Privilege
<b>Categories:</b>	4.6 DNS
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category II

### **Vulnerability Discussion:**

If an intruder gains control of named (BIND), then the intruder will acquire the privileges of the user ID under which it runs. Running as a non-privileged user account limits the extent of any breach. When BIND runs as SYSTEM (the default) intruders gain full control of the system.

### **Check:** DNS4530

The reviewer will validate ISC BIND is configured to run as a dedicated non-privileged service user account. Select the “Log On” tab of the properties of the ISC BIND service. If the ISC BIND service logs on as the “Local System account”, then this is a finding.



**Fix:** DNS4530

The SA should create a new user account dedicated to DNS, configure it per the DNS STIG, configure the ISC BIND service to logon as the new user account, and then restart the ISC BIND Service.

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

---

**Vulnerability Key:** V0003622

**STIG ID:** DNS4540

**Vulnerability:** The ISC BIND service user is a member of a group other than Everyone and Authenticated Users.

**IA Controls:** ECLP-1 Least Privilege

**Categories:** 2.2 Least Privilege

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:**

Membership in configurable groups gives the BIND service user unnecessary privileges that could be used by an intruder to further breach name server security.

**Check:** DNS4540

In Windows 2000/2003, select System Tools | Users and Groups | Users in the "Computer Management" tool. View the "Member Of" tab in the "User Properties" dialog Box (which can be accessed by double-clicking on the user). If the user is a member of any group besides "everyone" and "Authenticated Users", then this is a finding.

In Windows, a user does not have to be a member of any group other than the implicit groups "Everyone" and "Authenticated Users." Thus, to best ensure security, dnsuser must be removed from all explicit groups, including the "Users" group, into which all users are placed by default. There should not be a dnsgroup group as is recommended for UNIX.

**Fix:** DNS4540

The SA should remove the BIND service user account from all configurable user groups.

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:

**Vulnerability Key:** V0003623

**STIG ID:** DNS4550

**Vulnerability:** The ISC BIND service does not have the appropriate user rights required for the proper configuration and security of ISC BIND.

**IA Controls:** ECLP-1 Least Privilege

**Categories:** 2.2 Least Privilege

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:**

Having user rights beyond the minimum necessary gives the BIND service user unnecessary privileges that could be used by an intruder to further breach name server security.

**Check:** DNS4550

Windows 2000 adds several relevant user rights (actually user prohibitions). In “Local Security Settings” (a Microsoft Management Console Plug in), select Local Policies | User Rights Assignments in the left windowpane. By looking at the assignments in the right windowpane, check that the DNS user account is not listed under any assignments other than “Log on as a service,” “Deny access to this computer from the network,” and “Deny logon as batch job.” If the user has any additional rights beyond these, this is a finding.

**Fix:** DNS4550

The SA should grant the ISC BIND service the user rights of log on as service, Deny Access to This Computer from the Network, and Deny Logon as a Batch Job, which are required for the proper configuration and security of ISC BIND.

**OPEN:** ☐ **NOT** **APPLICABLE:** ☐ **FIXED:** ☐ **NOT A** **FINDING:** ☐

Comments:

**Vulnerability Key:** V0003624

**STIG ID:** DNS4570

**Vulnerability:** The appropriate encryption software is not correctly installed and configured on Windows ISC BIND name servers and it is required that in-band remote management be performed from hosts outside the enclave in which the name server resides.

**IA Controls:** ECCT-1 Encryption for Confidentiality  
ECCT-2 Encryption for Confidentiality

**Categories:** 8.1 Encrypted Data in Transit

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category II

**Vulnerability Discussion:**

If administrative network traffic is in the clear between external clients and name servers, then there is significant potential that authorized individuals can intercept and view that traffic, which may contain passwords and other sensitive information.

**Check:** DNS4570

The Systems Administrator may state that the evaluated Windows BIND name server is administered from a host outside of the internal network (e.g., a home office or remote site). In this case, there must be appropriate software on the Windows BIND name server to support encrypted communication. Once the service has been identified, the reviewer should check that the software does require encrypted sessions and authentication. Additional checks from the Secure Remote Computing STIG may apply. If the reviewer determines that the installed remote access/control configuration is inadequate, then there should be a finding with a written explanation specifying why the configuration is inadequate.

**Fix:** DNS4570

The IAO should prohibit in-band remote management until an appropriate network encryption solution has been deployed and tested.

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:



**Vulnerability Key:** V0003626

**STIG ID:** DNS4590

**Vulnerability:** The ownership and permissions on all Windows ISC BIND name servers are not as restrictive as required.

**IA Controls:** ECLP-1 Least Privilege

**Categories:** 2.2 Least Privilege

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category II

**Vulnerability Discussion:**

Weak permissions could allow an intruder to view or modify zone, configuration and/or program files.

**Check:** DNS4590

The reviewer can check permissions and ownership by looking at the properties of each file in “Windows Explorer.”

Note that there may be multiple zone files, key files, and log files. The reviewer should be able to produce a list of the files based on a quick examination of named.conf, which should have been obtained at the beginning of this module. The reviewer should check the permissions of each zone, key or log file when more than one exists on the name server.

The name of the root hints file is defined in named.conf. Common names for the root hints file are root.hints, named.cache, and db.cache.

<b><i>FOLDER/FILE NAME</i></b>	<b><i>OWNER</i></b>	<b><i>USER/GROUP</i></b>	<b><i>PERMISSIONS</i></b>
%systemroot%\system32\dns\bin	Administrators	Administrators	Full control
		dns-admins	Read
		dnsuser	Read
%systemroot%\system32\dns\etc	Administrators	Administrators	Full control
		dns-admins	Change
		dnsuser	Change
named.conf	Administrators	Administrators	Full control
		dns-admins	Change
		dnsuser	Read
named.pid	Administrators	Administrators	Full control
		dns-admins	Read
		dnsuser	Change
named.stat	Administrators	Administrators	Full control
		dns-admins	Read
		dnsuser	Change
root hints file	Administrators	Administrators	Full control
		dns-admins	Change
		dnsuser	Read
Any zone file	Administrators	Administrators	Full control
		dns-admins	Change
		dnsuser	Change
Any TSIG key file	Administrators	dnsuser	Read

If permissions are more permissive than required, then this is a finding.

**Fix:** DNS4590

The SA should modify permissions so that they are at least as restrictive as specified in the DNS STIG.

OPEN: ☐
 NOT APPLICABLE: ☐
 FIXED: ☐
 NOT A FINDING: ☐

Comments:

---

## 4. WINDOWS DNS

<b>Vulnerability Key:</b>	V0012479
<b>STIG ID:</b>	DNS0260
<b>Vulnerability:</b>	Computer accounts for DHCP servers are members of the DNSUpdateProxy group.
<b>IA Controls:</b>	ECLP-1 Least Privilege
<b>Categories:</b>	4.6 DNS
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category II

### Vulnerability Discussion:

A built-in security group, DNSUpdateProxy, is provided as of Windows 2000. This group can update DNS records for clients without becoming the owner of the records. When DHCP servers are added as members of this group, any of the (member) DHCP servers can update the records. The first user that is not a member of the DNSUpdateProxy group to modify the records associated with a client; becomes the owner. There is a vulnerability for all servers (even non-domain controllers) on which a DHCP service runs. The DNS records associated with the DHCP server host could be modified by other DHCP servers that are members of the DNSUpdateProxy group. In order to prevent this from occurring, DHCP should not be installed on a domain controller if the group DNSUpdateProxy is utilized.

### Check: DNS0260

Review the membership of the DNSUpdateProxy group to determine if any of the computer accounts are DHCP servers. If there are any computer accounts for DHCP servers, this is a finding.

View Computer Management, Local Users and Groups, Groups. Review the membership of the DNSUpdateProxy group to determine if any of the accounts are DHCP servers.

On domain controllers, run the active directory users and computers snap-in to verify the DNSUpdateProxy group. Select, Start->Run->dsa.msc.

### Fix: DNS0260

The IAO will ensure computer accounts for DHCP servers are not members of the DNSUpdateProxy group.

**OPEN:** ☐

**NOT  
APPLICABLE:** ☐

**FIXED:** ☐

**NOT A  
FINDING:** ☐

Comments:

---



<b>Vulnerability Key:</b>	V0004501
<b>STIG ID:</b>	DNS0805
<b>Vulnerability:</b>	The DHCP server service is not disabled on any Windows 2000/2003 DNS server that supports dynamic updates.
<b>IA Controls:</b>	ECCD-1 Changes to Data ECCD-2 Changes to Data
<b>Categories:</b>	4.6 DNS
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category I

**Vulnerability Discussion:**

There is a significant vulnerability potential when the DHCP service runs using the computer account of a Windows Domain Controller, as in the default Windows configuration. This account has full control over all DNS objects stored in Active Directory. In this case, the DHCP server has access to modify the SRV (and other) records for all the Domain Controllers. When these records were replicated to other domain controllers (when AD Integrated DNS is used as required by the STIG), all the Windows DNS servers could potentially be compromised.

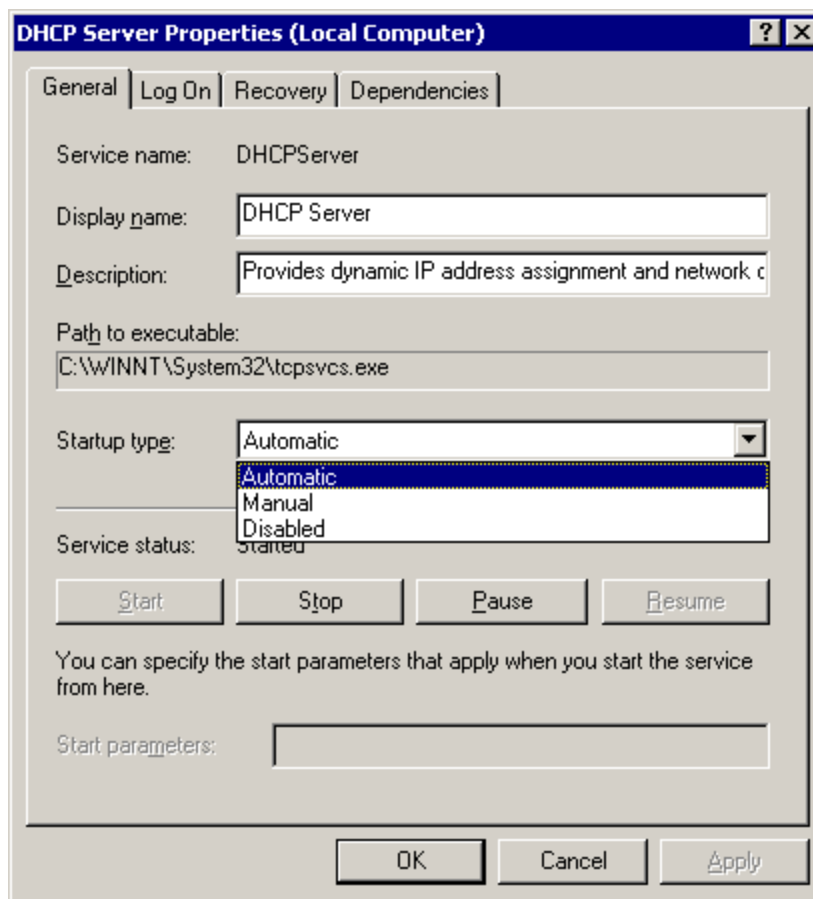
**Check:** DNS0805

Log in to the server with an account that has admin rights. Right-click “My Computer” on the desktop and click “Manage.” This brings up the “Computer Management” tool.

Click the plus sign next to “Services and Applications” on the left pane to expand it. Select “Services” on the left panel.

On the right pane, scroll down and select “DHCP Server.” Right-click “DHCP Server” and click “Properties.” This brings up the “DHCP Server Properties”.

The reviewer will validate the DHCP server service is disabled. The “Disabled” drop down selection is to be selected on the “General” tab of the “DHCP Server Properties.” If the DHCP server service is not disabled, then this is a finding.



**Fix:** DNS0805

Working with appropriate SA and technical personnel, the IAO should plan to migrate the DHCP service to another machine as soon as it is feasible to do so.

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

**Vulnerability Key:** V0004502

**STIG ID:** DNS0810

**Vulnerability:** Zone transfers are not prohibited or a VPN solution is not implemented that requires cryptographic authentication of communicating devices and is used exclusively by name servers authoritative for the zone.

**IA Controls:** DCNR-1 Non-repudiation – Cryptography Standard

**Categories:** 4.6 DNS

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category I

**Vulnerability Discussion:**

If zone transfers are not cryptographically authenticated, then there is the potential for an adversary to masquerade as a legitimate zone partner and update zone records without authorization.

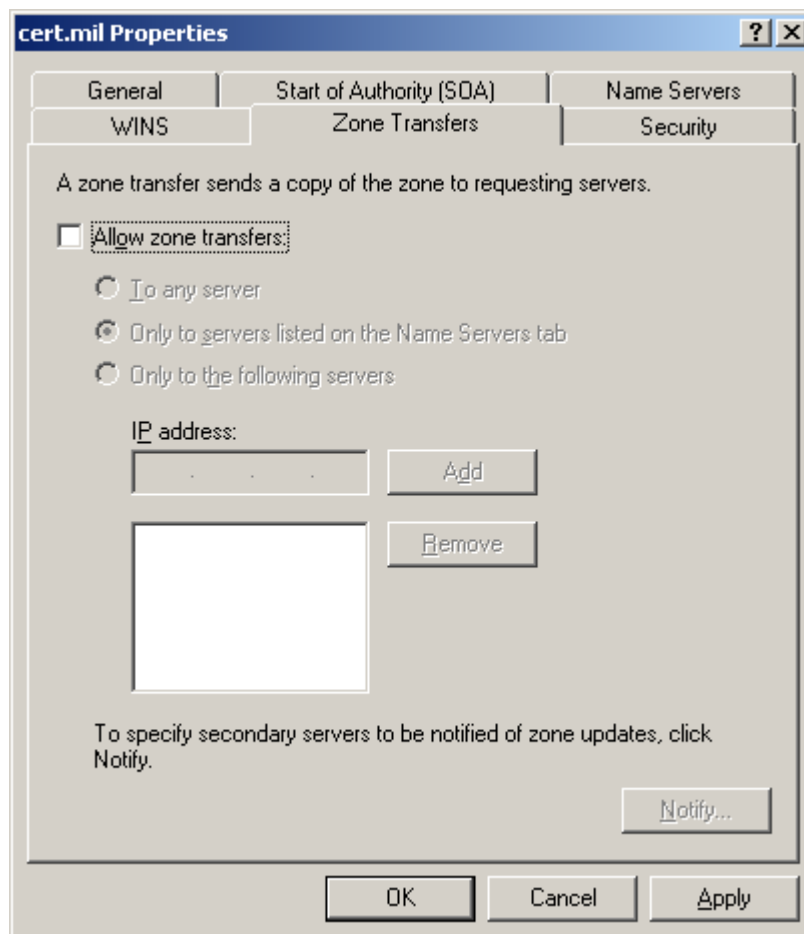
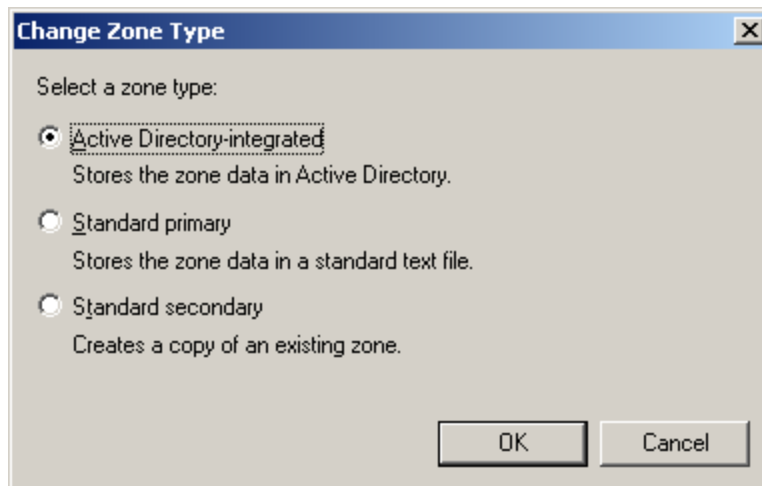
**Check:** DNS0810

The reviewer will validate zone transfers are prohibited. The reviewer will ensure the "Allow zone transfers" check box is not selected on the "Zone Transfers" tab of the name server properties.

If zone transfers are allowed, then this is a finding.

Windows allows for two ways of synchronizing zone data across name servers: (1) traditional RFC-compliant DNS zone transfers; and (2) AD-replication. The latter only works when Windows DNS is integrated with AD, which makes each of the DNS records an AD object. The Windows 2000/2003 DNS implementation of traditional zone transfers does not meet the STIG requirement that the transfers be cryptographically authenticated using a technology such as TSIG. Fortunately, AD-replication is cryptographically authenticated. Therefore, the solution in a pure Windows 2000/2003 DNS implementation is to integrate DNS with AD and disable zone transfers.





**Mitigation:**

All of the following must apply:

- All DNS servers are in a secured Enclave with all appropriate network infrastructure protections and communicate strictly behind the perimeter, or on a non-contiguous network where the public links between site segments are protected with site-to-site VPNs

- Such network is completely controlled by the server owner
- Access to the network is protected IAW the network infrastructure STIG
- Access to the DNS servers and resources is limited to members and servers of the DNS server owner's organization

If all of the aforementioned requirements are met, this finding can be downgraded to a CAT II.

**Fix:** DNS0810

Working with relevant DNS administrators, the SA should configure Windows DNS to rely on Active Directory to replicate zone data whenever possible. If this is not feasible, then the SA must establish an IPSEC VPN between relevant zone partners or implement a satisfactory alternative encryption-based authentication technology.

OPEN: ☐      NOT APPLICABLE: ☐      FIXED: ☐      NOT A FINDING: ☐

Comments:

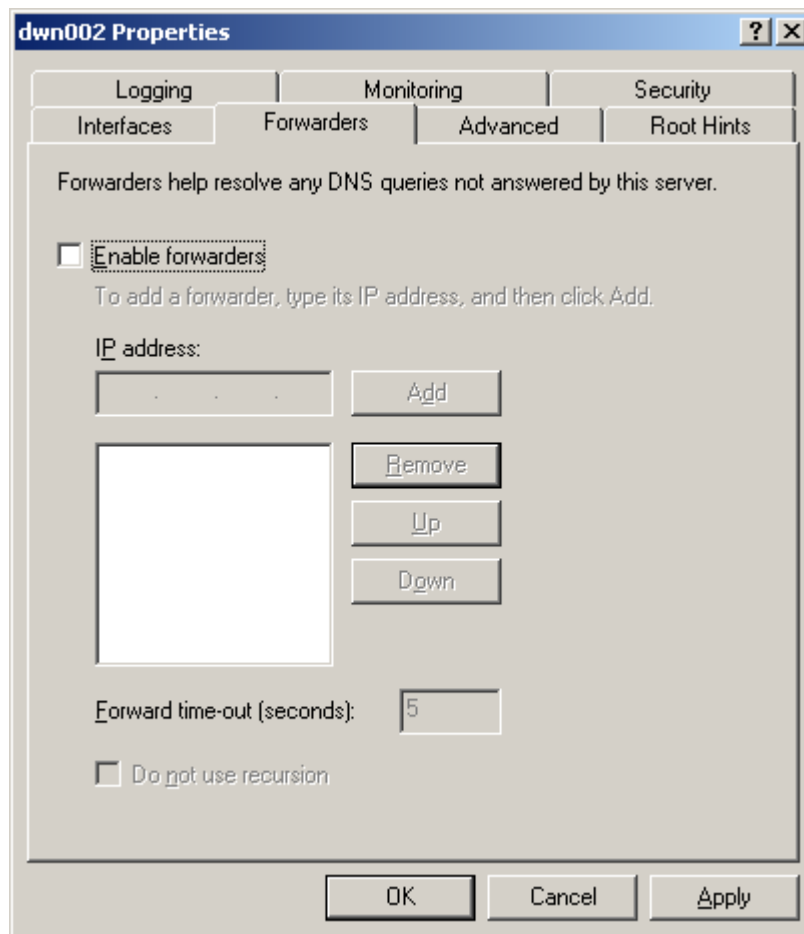
<b>Vulnerability Key:</b>	V0004503
<b>STIG ID:</b>	DNS0815
<b>Vulnerability:</b>	Forwarders on an authoritative Windows 2000/2003 DNS server are not disabled.
<b>IA Controls:</b>	ECSC-1 Security Configuration Compliance
<b>Categories:</b>	4.6 DNS
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category II

**Vulnerability Discussion:**

Windows DNS has historically been more vulnerable to cache poisoning attacks than BIND. The algorithm used for answering recursive queries also makes it more prone to self-imposed denial of service attacks and as an amplification device for attacks on other DNS servers. Additionally, Windows DNS does not allow for the fine-grained access control restrictions (i.e., limiting the clients that are able to perform recursion) that are allowed by BIND and other recursive DNS appliances. Therefore, Windows 2000/2003 DNS should not be deployed as a caching name server. Consequently, the use of forwarders and recursion is prohibited on Windows 2000/2003 DNS servers.

**Check:** DNS0815

Windows DNS should not be deployed as a caching name server. Consequently, the use of forwarders and recursion is prohibited on external Windows 2000/2003 DNS. The reviewer will validate that the "Enable Forwarders" check box is not selected on the "Forwarders" tab of the name server properties.



If forwarders are enabled, then this is a finding.

**Fix:** DNS0815

The SA should disable forwarding (on the Forwarders tab of the name servers properties dialog box).

OPEN: ☐ NOT APPLICABLE: ☐ FIXED: ☐ NOT A FINDING: ☐

Comments:

\

**Vulnerability Key:** V0004505

**STIG ID:** DNS0825

**Vulnerability:** WINS lookups is not prohibited on a Windows 2000/2003 DNS server.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 4.6 DNS

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category I

**Vulnerability Discussion:**

Integration of WINS and Windows 2000/2003 DNS leaves Windows DNS open to all the vulnerabilities of WINS, including the ability to update records without authentication.

**Check:** DNS0825

The reviewer will validate the "Use WINS forward lookup" is not checked on the "WINS" tab on the properties dialog of each zone.

If WINS is integrated on a Windows 2000/2003 DNS server, then this is a finding.

**Fix:** DNS0825

The SA should disable any integration between DNS and WINS as soon as it feasible to do so. If WINS is required for legacy applications, then DNS clients will need to be reconfigured to use WINS rather than DNS for NetBIOS name resolution. The SA should uncheck Use WINS forward lookup on the WINS tab on the properties dialog of each zone.

**OPEN:** ☐      **NOT APPLICABLE:** ☐      **FIXED:** ☐      **NOT A FINDING:** ☐

Comments:

**Vulnerability Key:** V0003625

**STIG ID:** DNS4580

**Vulnerability:** Shares other than the default administrative shares are enabled on a name server.

**IA Controls:** ECAN-1 Access for Need-to-Know

**Categories:** 2.2 Least Privilege

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category II

**Vulnerability Discussion:**

Non-administrative shares are unnecessary for name server operation and provide adversaries with an additional possible point of attack.

**Check:** DNS4580

From a command prompt, type `net share` and press enter. If any shares appear other than default administrative shares (e.g., C\$, NETLOGON\$), then this is a finding

**Fix:** DNS4580

The SA should disable all non-administrative shares.

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:

**Vulnerability Key:** V0014768

**STIG ID:** DNS4630

**Vulnerability:** The IPv6 protocol is installed and the server is only configured to respond to IPv4 A records.

**IA Controls:** ECSC-1 Security Configuration Compliance

---

<b>Categories:</b>	4.6 DNS
<b>Responsibility:</b>	DNS Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category II

**Vulnerability Discussion:**

To prevent the possibility of a denial of service in relation to an IPv4 DNS server trying to respond to IPv6 request, the server should be configured to not listen on any of its IPv6 interfaces unless it does contain IPv6 AAAA resource records in one of the zones.

**Check:** DNS4630

*Windows*

- Instruction: Click **Start**, click **All Programs**, click **Administrative Tools**, and select **DNS**. Expand the **Forward Lookup Zones** folder. Expand each zone and check for IPv6 records. If all records are IPv4, then confirm IPv6 is not enabled on any of the lan interfaces with the following:
  - Click **Start**, click **Control Panel**, and the double-click **Network Connections**.
  - Right-click any local area connection, and then click **Properties**.
  - The display will contain, **Microsoft TCP/IP version 6** with a check next to the item if IPv6 is installed.

**Fix:** DNS4630

The DNS administrator will uninstall IPv6 from any lan interface that is not hosting IPv6 AAAA records within its zones. The following steps should be followed to uninstall IPv6 on an interface:

- Click **Start**, click **Control Panel**, and the double-click **Network Connections**.
- Right-click any local area connection, and then click **Properties**.
- The display will contain, **Microsoft TCP/IP version 6** with a check next to the item if IPv6 is installed.
- Select **Microsoft TCP/IP version 6** and then click **Uninstall**.
- Select **Yes** to confirm the removal.
- Select **Yes** restart the computer for the new settings to take effect.



**OPEN:** ☐      **NOT APPLICABLE:** ☐      **FIXED:** ☐      **NOT A FINDING:** ☐

Comments:

## 5. CISCO CONTENT SWITCH

<b>Vulnerability Key:</b>	V0004506
<b>STIG ID:</b>	DNS0900
<b>Vulnerability:</b>	The shared secret in the APP session(s) was not a randomly generated 32 character text string.
<b>IA Controls:</b>	DCNR-1 Non-repudiation – Cryptography Standard
<b>Categories:</b>	8.4 Key Management
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category III

### Vulnerability Discussion:

The core requirements related to zone transfers are that an authoritative name server transfers zone information only to designated zone partners and that name servers only accept zone data when it is cryptographically authenticated. CSS APP provides means to designate with which devices it can share zone data and to authenticate those transactions. CSS devices can define their peers using IP addresses and authenticate them using Challenge Handshake Authentication Protocol (CHAP) with a shared secret. This setup also can be supplemented with MD5 hashing encryption. While this configuration does not provide the equivalent strength of cryptographic authentication as BINDs TSIG HMAC-MD5, it does provide a satisfactory level of information assurance when CSS DNS operates within a trusted network environment.

### Check: DNS0900

Interview the SA and determine if the key was a randomly generated 32-character text string.

### Fix: DNS0900

The CSS DNS administrator should use the following command while in global command mode; app session ip\_address authChallenge shared\_secret encryptMd5hash. In this command, ip\_address refers to the IP address of the designated peer and the shared\_secret is a text string up to 32 characters in length.

OPEN: <input type="checkbox"/>	NOT APPLICABLE: <input type="checkbox"/>	FIXED: <input type="checkbox"/>	NOT A FINDING: <input type="checkbox"/>
--------------------------------	--	---------------------------------	---

Comments:

**Vulnerability Key:** V0004507

**STIG ID:** DNS0905

**Vulnerability:** The Cisco CSS DNS is utilized to host the organizations authoritative records and DISA Computing Services does not support that host in its csd.disa.mil domain and associated high-availability server infrastructure.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 4.6 DNS

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category II

**Vulnerability Discussion:**

The primary security concern with regard to the type of delegation discussed is that to implement this approach, an organization would have to migrate its authoritative records from a well-known DNS implementation with proven, tested security controls to a relatively new DNS implementation without similar controls. Therefore, this migration should only occur when the performance and availability advantages of CSS significantly outweigh the increased residual security risk of using a less mature technology.

**Check:** DNS905

Determine whether the CSS DNS device is used as an authoritative name server. If the CSS DNS does maintain authoritative records, then this is a finding. The exception to this is if this CSS DNS device supports authoritative records for a host(s) within the csd.disa.mil domain, which is not a finding.

Instruction: In the presence of the reviewer, the CSS DNS administrator should enter the following command while in global configuration mode:

show dns-record statistics

If any of the hosts have domain names outside of the csd.disa.mil domain, then this is a finding.

**Fix:** DNS0905

The CSS DSN administrator should use the following command while in global command mode; no dns-record, to remove domain records that do not support hosts in the csd.disa.mil domain.

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:

**Vulnerability Key:** V0004508

**STIG ID:** DNS0910

**Vulnerability:** Zones are delegated with the CSS DNS.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 4.6 DNS

**Responsibility:** Information Assurance Officer

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:**

Although it is technically possible to delegate zones within CSS DNS, there is almost never a rationale to do so because such delegation could be achieved as easily with BIND, which offers security features not present in CSS DNS. Moreover, the performance enhancing features of CSS typically would not apply to name server records because these records are obtained easily and quickly across the wide area without significant impact on a users experience

**Check:** DNS910

In the presence of the reviewer, the CSS DNS administrator should enter the following command while in global configuration mode:

```
show dns-record statistics
```

There should be no DNS record types of NS. If there are NS records, then this is a finding.

**Fix:** DNS0910

The CSS DNS administrator should remove any NS records with the following command while in global configuration mode; no dns-record ns domain\_name.

<b>OPEN:</b>	<input type="checkbox"/>	<b>NOT APPLICABLE:</b>	<input type="checkbox"/>	<b>FIXED:</b>	<input type="checkbox"/>	<b>NOT A FINDING:</b>	<input type="checkbox"/>
--------------	--------------------------	----------------------------	--------------------------	---------------	--------------------------	---------------------------	--------------------------

Comments:

<b>Vulnerability Key:</b>	V0004512
<b>STIG ID:</b>	DNS0915
<b>Vulnerability:</b>	CSS DNS does not cryptographically authenticate APP sessions.
<b>IA Controls:</b>	DCNR-1 Non-repudiation
<b>Categories:</b>	4.6 DNS
<b>Responsibility:</b>	System Administrator
<b>References:</b>	DNS STIG
<b>Severity:</b>	Category I

**Vulnerability Discussion:**

The risk to the CSS DNS in this situation is that the CSS DNS peers do not authenticate each other, the sending and receiving of APP session data and peer communication may be with an adversary rather than the intended peer, thereby sending sensitive network architecture data and receiving ill intended zone data. To protect against this possibility, the CSS DNS peers must cryptographically authenticate each other.

**Check:** DNS0915

In the presence of the reviewer, the CSS DNS administrator should enter the following command while in global configuration mode:

```
show app session
```

Confirm the authentication type is set to “authChallenge” and the encryption type is set to “encryptMd5hash.” This will confirm APP CHAP authentication and MD5 hashing features for APP sessions are configured between peers, if this is not the case, then this is a finding. The only exception would be if the CSS DNS administrator uses an IPSEC VPN between each peer couple. Review the IPSEC VPN with the CSS DNS administrator and validate the IPSEC VPN is configured between peers, if this is not the case, then this is a finding.

**Fix:** DNS0915

The command, show app session, displays that the authentication type is not set to authChallenge and the encryption type is not set to encryptMd5hash.

Comments:

**Vulnerability Key:** V0004509

**STIG ID:** DNS0920

**Vulnerability:** The CSS DNS does not transmit APP session data over an out-of-band network if one is available.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 4.6 DNS

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:**

One can also limit APP communication to an out of band network, which would make it considerably more difficult for adversaries to spoof the addresses of peers or hijack APP sessions.

**Check:** DNS0920

In the presence of the reviewer, the CSS DNS administrator should enter the following command while in global configuration mode:

show app session

Instruction: Ensure Application Peering Protocol (APP) session data is not sent over an out-of-band network. If APP session data is sent over an out-of-band network, then this is a finding.

**Fix:** DNS0920

The CSS DNS administrator should use the following command while in global configuration mode; app session 1.2.3.4 (sample IP address), to configure CSS to only transmit session data over an out-of-band network, if one is available.

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:

**Vulnerability Key:** V0004510

**STIG ID:** DNS0925

**Vulnerability:** Forwarders are not disabled on the CSS DNS.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 4.6 DNS

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category II

**Vulnerability Discussion:**

CSS DNS is not vulnerable to attacks associated with recursion because it does not support recursion, but does offer a forwarder feature that sends un-resolvable or unsupported requests to another name server. This feature poses a risk because the forwarder feature merely redirects potential attacks to another name server.

**Check:** DNS0925

In the presence of the reviewer, the CSS DNS administrator should enter the following command while in global configuration mode:

```
show dns-server forwarder
```

Confirm the DNS server forwarder primary and DNS server forwarder secondary are “Not Configured.” If either of these is configured, then this is a finding.

**Fix:** DNS0925

The CSS DNS administrator should disable forwarders by entering the following command while in global configuration mode: no dns-server forwarder primary (if a primary) or no dns-server forwarder secondary (if a secondary).

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:

**Vulnerability Key:** V0004467

**STIG ID:** DNS0225

**Vulnerability:** DNS database administrators with the assistance of record owners will validate the zone records annually. The DNS database administrator will remove all zone records that are not validated each year.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 4.6 DNS

**Responsibility:** Information Assurance Officer

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:**

If zone information has not been validated in over a year, then there is no assurance that it is still valid. If invalid records are in a zone, then an adversary could potentially use their existence for improper purposes. An SOP detailing this process can resolve this requirement.

**Check:** DNS0225

The reviewer should check that the record's last verified date is less than one year prior to the date of the review. If this is not the case for any host or group of hosts, then this is a finding.

**Fix:** DNS0225

Working with DNS Administrators and other appropriate technical personnel, the IAO should attempt to validate the hosts with expired validation dates. If these cannot be validated within a reasonable period of time, they should be removed.

A zone file should contain adequate documentation that would allow an IAO or newly assigned administrator to quickly learn the scope and structure of that zone. In particular, each record (or related set of records, such as a group of LAN workstations) should be accompanied by a notation of the date the record was created, modified, or validated and record the owner's name, title, and organizational affiliation. The owner of a record is an individual with the authority to request that the record be modified or deleted.

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:



**Vulnerability Key:** V0004469

**STIG ID:** DNS0235

**Vulnerability:** Zone-spanning CNAME records, that point to a zone with lesser security, are active for more than six months.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 4.6 DNS

**Responsibility:** System Administrator

**References:** DNS STIG

**Severity:** Category III

**Vulnerability Discussion:**

The use of CNAME records for exercises, tests or zone-spanning aliases should be temporary (e.g., to facilitate a migration). When a host name is an alias for a record in another zone, an adversary has two points of attack the zone in which the alias is defined and the zone authoritative for the aliases canonical name. This configuration also reduces the speed of client resolution because it requires a second lookup after obtaining the canonical name. Furthermore, in the case of an authoritative name server, this information is promulgated throughout the enterprise to caching servers and thus compounding the vulnerability.

**Check:** DNSS0235

Review the zone files and the DNS zone record documentation and confirm that there are no CNAME records older than 6 months. If there are CNAME records older than 6 months, then this is a finding.

**Fix:** DNS0235

The DNS database administrator should remove any zone-spanning CNAME records that have been active for more than six months.

**OPEN:** ☐ **NOT APPLICABLE:** ☐ **FIXED:** ☐ **NOT A FINDING:** ☐

Comments:

## 6. SUMMARY OF CHANGES

15 March 2008

DNS0190 corrected vulnerability key to V0012364.

DNS0200 removed “geographically dispersed” from the requirement.

DNS0402 corrected vulnerability key to V0014763.

DNS0402 added guidance for windows with/without BIND.

DNS0425 removed duplicate “or dns.exe”.

DNS0425 clarified guidance for and standard and active-directory integrated zones.

DNS0435 emphasized “NOT” in the vulnerability description.

DNS0460 deleted “Those integrated with active directory should be marked not a finding” from windows guidance.

DNS0475 clarified the Forwarders Tab can only be found on Windows 2000.

DNS0490 clarified windows guidance to also check debug log files.

DNS0710 removed file permissions from the requirement.

DNS4650 corrected the algorithm number for RSASHA1 to be five and not one.

DNS4670 corrected vulnerability discussion.

DNS4480 corrected tables for log files and TSIG keys.

DNS4580 changed command from net view to net share.

15 May 2008

EN0540 Added additional windows guidance.

DNS0225 corrected typo “he” with “The”

DNS0420 moved “Windows DNS with AD should be marked NA” into the check portion

DNS0440 removed requirement for checking ntds.dit.

DNS0460 clarified check is for traditional DNS zones on Windows.

DNS0485 updated “Notify” to “Notifications”

DNS0260 added guidance for domain accounts.

DNS4580 removed 127.0.0.1 from net share command.

15 September 2008

DNS0815 removed requirement for external servers only.

15 December 2008

DNS0190 corrected vulnerability key.

15 June 2009

DNS0450 added language for deny by default for BIND allow-updates clause.

15 August 2009

DNS0402 updated required minimum versions to reflect IAVA 2009-A-0060.

This page is intentionally left blank.